FUNDAMENTOS DE LA INFORMÁTICA FORENSE

JOCSAN LAGUNA

Todo comienza con un sueño…

Índice

Introducción	6
1. Procesos de la informática forense	8
1.1 Identificación	9
1.2 Preservación	9
1.2.1 Colisión de evidencia digital	13
1.3 Análisis	23
1.4 Presentación	23
2. Tipos de análisis forenses	25
2.1 La teoría del fruto del árbol envenenado	26
3. Recolección de evidencia	29
3.1 Antes de iniciar	30
3.2 Diferencias entre copia forense y backup	31
3.3.1 Memoria RAM en sistemas Windows	33
3.3.2 Memoria RAM en Linux	38
3.4 Comandos de Windows como herramientas forenses	42
3.4.1 Tablas de protocolo ARP	43
3.4.2 Historial de CMD	44
3.4.3 Configuración de red en Windows	45
3.4.4 Conexiones activas en Windows	46
3.4.5 Tareas programadas	48
3.4.6 Información del sistema	49
3.5 Historial de navegadores	49
3.6 Utilidades	51
3.6.1 Agave	52
3.6.2 WinTriage	53
3.6.3 WinUFO	55
4. Copia forense	57
4.1 Tipos de copias forenses	57
4.2 Formatos de copias forenses	58
4.3 Principales retos	60
4.4 Hardware de informática forense	66
4.4.1 Bloqueadores de escritura	66
4.4.2 Duplicadores	68
4.5 Copia forense de discos duros	70
4.5.1 Copia forense con FTK Imager	70

4.5.2 Copia forense con OSForensic	78
4.5.3 Copia forense con HelixPro	80
4.6 Copia forense desde Linux	82
4.7 Copia forense en vivo, sistemas Windows	84
4.7.1 Detección de unidades cifradas	86
4.7.2 Copia forense en vivo, entornos Windows cifrados	93
4.8 Cálculo de hash en Windows	96
4.8.1 CMD	96
4.8.2 PowerShell	97
4.8.3 Multihasher	97
4.8.4 OSForensic	98
4.9 Cálculo de hash en Linux	99
5. Laboratorio forense	101
5.1 Suite y distribuciones forenses	103
5.2 Autopsy Forensic	104
5.2.1 Crear un caso	105
5.2.2 Agregar evidencia	108
5.2.3 Módulos	110
5.2.4 Visualización de evidencia	113
5.2.5 Timeline	117
5.3 Suite forense comercial	118
6. Investigación digital sobre Windows	124
6.1 Agregar evidencia	124
6.2 Montaje de copias forenses	128
6.3 Usuarios existentes	133
6.4 Host	137
6.5 Eventos del sistema	139
6.6 Prefetch	141
6.7 Shadowcopy	143
6.8 MFT	146
7. Análisis de la memoria RAM	149
7.1 Volatility	149
7.1.1 Perfiles	150
7.1.2 Procesos y subprocesos	151
7.1.3 Inspección de librerías usadas	153
7.1.4 Extracción de ejecutables	154
Índice de ilustraciones	156
Credenciales para informática forense	159

Laboratorios Forenses	160

Introducción

El mundo de la informática forense me ha resultado siempre apasionante, no solo por el hecho de que la parte tecnológica y la legal se tocan, sino porque a lo largo de los años he visto que quien conoce y maneja estas dos áreas, sobresale en el sector. Casos que he llevado en más de una década de investigaciones son muchos, desde aquellos en donde buscamos solo detectar si empleados están robando información en un corporativo, ataques informáticos a servidores críticos que se desconoce si es interno o externo el vector de ataque, hasta casos mediáticos en donde una persona es acusada de delitos graves como violación, homicidio o secuestro, siendo el dispositivo celular la pieza clave que puede inclinar la balanza para uno u otro lado y permitir que la justicia se haga presente.

A lo largo de las siguientes páginas, abordaremos las técnicas y el protocolo de acciones ordenadas para llevar a cabo procesos de informática forense, pero muy importante, hablaremos de porqué de cada una de las técnicas y normas según sea el caso, de igual forma trataremos los puntos clave para dar certeza que los elementos que extraemos son una copia integra de los originales, y las conclusiones a las que llegamos después de procesar la información son reales, dejando registro que nada ha sido manipulado más allá de lo estrictamente necesario y que con cualquier otra herramienta gratuita o

de paga, otro experto podría replicar nuestros mismos resultados. Estos serán los fundamentos de la informática forense, como veremos en su momento, cuando se presenta una investigación de informática forense, muchas veces por el valor y las consecuencias de nuestro reporte de resultados, se deriva en despidos, acciones legales o reestructuraciones dentro de corporativos, por ello, el derecho a réplica es bastante común, siendo necesario cuidar que nuestras investigaciones estén guiadas siempre por las mejores prácticas.

El enfoque del libro está pensando gente de sistemas y abogados que se quieren especializar en temas de informática, partiremos con sólidos conocimientos de normas y leyes para adentrarnos en la parte técnica de extraer la evidencia y procesarla.

1. Procesos de la informática forense

El punto angular de una investigación de informática forense es siempre la preservación del escenario inicial, esto es algo que desde ya quiero hacer hincapié; la parte legal resultará clave si quieren dedicarse de lleno a la informática forense o cuando menos, si estarán trabajando en un corporativo, estén tranquilos que sus investigaciones podrán ser soportadas en un proceso judicial si se llegase a requerir.

Quisiera compartirles como ejemplo, que si en una empresa se detectó que un empleado estaba robando información de marcas, patentes, estrategias de marketing y toda la evidencia es obvia, si al llevar a cabo el proceso de preservación de evidencia se omitieron los pasos clave, la investigación no tendrá valor frente a las autoridades… esto es algo que veo muy seguido cuando me toca defender a un empleado y observo que la preservación omitió pasos, en un juicio basta solo señalar por que la trazabilidad de la evidencia está en duda, para que un juez dictamine que no puede ejercer una acción cuando de la evidencia ya quedó cuestionada su inmutabilidad.

El tema de ¿cómo comenzar y que pasos debo seguir en mis investigaciones? La mejor respuesta es que cada caso se analiza en concreto, sin embargo, de forma general hay modelos de trabajo, uno de las que a mi consideración es sencillo y muy práctico al momento de aplicarlo, es el

desarrollado por el U.S. Dep. of Justice (2001), en donde el proceso de investigación informática se divide en 4 pasos:

- **Identificación**
- **Preservación**
- **Análisis**
- **Presentación**

1.1 Identificación: Aquí entra la parte del analista (nosotros), que, tras conocer los detalles del caso, decidiremos que equipos tecnológicos formarán parte de nuestra investigación, que instancias de la nube serán requeridas, que servidores serán solicitados o si nos vamos a llevar o no el router para analizarlo, esta parte es delicada ya que seremos nosotros los que indicaremos que se analiza y que puede ser excluido.

1.2 Preservación: Este a mi perspectiva es el corazón de una investigación cuyo resultado se presentará ante una autoridad o existe la posibilidad de un contra peritaje informático, ya que aquí es donde un segundo investigador revisará con lupa cualquier error u omisión en el proceso, consiguiendo con ello desvirtuar cualquier resultado que pueda arrojar el análisis.

Existe un concepto legal que se conoce como cadena de custodia, este procedimiento controlado, es el que nos va a permitir darle trazabilidad a cada uno de los elementos que como investigadores tengamos disponibles, ya que la

cadena de custodia, en el campo de la informática, registra desde que un archivo fue extraído de un equipo de cómputo, pasando por validar la integridad del mismo, y además una certeza científica que permita que tras pasar de manos la evidencia, se pueda comprobar que el archivo continua integro (o no) tal y como fue extruido desde un inicio. Un ejemplo dentro de otra área sería una escena del crimen en donde un cuchillo fue encontrado, debe existir un registro controlado señalando quien lo encontró y recolectó, a quien le fue entregado por primera vez, si este se le entregó a otra persona y hasta la última persona que lo tuvo en sus manos, eso sería la cadena de custodia, el documento que soporta el orden de todos los que estuvieron resguardando la evidencia, podría ser verificado si el cuchillo que tiene la última persona, es el mismo que recolectó la primera, ya que fue detallado en un inicio el tamaño, colores, características… el ejemplo queda claro, pero ahora en el mundo de la informática nos preguntamos, ¿cómo puedo validar que un archivo que se está analizando no ha sido alterado o modificado a lo largo del tiempo? En este punto, en la rama de la informática lo que nos permitirá registrar la cadena de custodia, se le denomina “valor de integridad hash”, el cual será de aquí y hasta el final del libro, el elemento que tendremos que registrar unas veces si y otras veces también, dicho de otra forma, siempre se debe tener el registro de ese valor, no entraremos en este libro a la parte técnica del proceso técnico detrás de estos valores, ya que daría para un libro

de algoritmos y programación, muy alejado de nuestro objetivo que es la preservación de evidencia.

Dejando muchas cosas técnicas en el tintero, para fines de comprensión de este concepto veamos el valor de integridad hash como un número de serie asociado a un elemento digital, el elemento digital puede ser un archivo de Word, Excel, PowerPoint, una foto, video, audio, pdf, archivo HTML, o bien, algo más práctico, un valor de integridad hash puede ser de un disco duro completo, incluyendo todas sus particiones y cientos de miles de archivos que este contenga; el valor de integridad hash lo podemos generar sobre cualquier elemento o elementos digitales que tengamos disponibles.

De los algoritmos usados para el cálculo de estos valores de integridad hash, podemos poner un ejemplo calculando de la palabra “hola” el valor de integridad hash respectivo sería:

MD5: d41d8cd98f00b204e9800998ecf8427e

SHA-1: da39a3ee5e6b4b0d3255bfef95601890afd80709

SHA-256:
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca
495991b7852b855

Después de los dos puntos, la secuencia de números y letras que se observan, son el valor de integridad hash bajo

el algoritmo correspondiente, cada uno de estos algoritmos tiene ventajas y desventajas que serán cruciales, por lo que veremos sus similitudes y diferencias

Similitudes:

- Son empleados los números del 0-9 y las letras de la A-F
- La secuencia de números tiene una extensión limitada, no importa que el valor de integridad hash se calcule de un archivo de 1 Kb o de un disco duro con 100,000 Tb, el valor de integridad hash será siempre de una extensión de acuerdo con el algoritmo.

El hecho de que el valor de integridad hash use además de números, letras, hace que las probabilidades de que dos elementos totalmente distintos coincidan con el valor de integridad hash sea casi imposible.

Del ejemplo anterior podemos tomar el valor MD5: d41d8cd98f00b204e9800998ecf8427e, el primer valor es la letra “d”, este primer valor pudo haber sido un número del 0-9 ó una letra de la A-F (eso se conoce como valores hexadecimales), esto implica que existen 16 opciones para el primer valor y se repite con el segundo y hasta el último de los caracteres del valor de integridad hash.

Diferencias:

- La extensión del MD5 se tiene por 32 caracteres, del SHA-1 a 40 caracteres y el algoritmo SHA-256 con 60 caracteres.

La probabilidad de coincidencia de dos valores hash se calcula elevando 16 (cada una de las posibilidades que tiene cada uno de los valores) a la potencia correspondiente (el número de caracteres de cada algoritmo)

- ✓ MD5: Con probabilidad de coincidencia 16 ^ 32 = 3.402823669209384634633746074317 7e+38
- ✓ SHA-1 Con probabilidad de coincidencia 16 ^ 40 = 1.461501637330902918203684832716 3e+48
- ✓ SHA-256 Con probabilidad de coincidencia 16 ^ 64 = 1.766847064778384329583297500742 9e+72

IMPORTANTE: Dado que es una pregunta que usualmente me hacen, aclaro que calcular un valor de integridad hash no incrusta ese valor sobre un documento, no lo certifica ni lo modifica, es solo obtener del documento, un por decirlo así, número de serie que debe ser único.

1.2.1 Colisión de evidencia digital

Con estas probabilidades de coincidencia, se podría pensar que se puede usar de forma indistinta cualquiera de

los algoritmos, sin embargo, para fines de rendir un reporte ante una autoridad y dar certeza científica, el algoritmo MD5 y SHA-1, no deben ser empleados, la razón es muy simple, desde hace años se publicó y demostró que dos archivos totalmente distintos, pueden tener intencionalmente el mismo valor MD5, de igual forma se demostró que para el algoritmo SHA-1, se puede realizar el mismo proceso, de generar dos archivos totalmente distintos con el mismo valor SHA1, a esto se le conoce como colisión hash.

Para fines de comprender la importancia y relevancia de las colisiones en los algoritmos MD5 y SHA-1, una analogía muy sencilla es imaginar dos casquillos de proyectil, uno de 9 mm y otro de 50 mm, evidentemente solo con verlos se sabe que corresponden a armas de fuego distintas, pero con este concepto en mente de “colisión hash”, es como si el número de evidencia dentro de un proceso legal fuera el mismo. Esto es lo que en informática implica que se usen algoritmos MD5 o SHA-1, los cuales ya se demostró que tienen colisiones, no se puede probar que el elemento digital que esté analizando, no ha sido manipulado.

Veamos esto con un ejemplo gráfico, a continuación, presento dos imágenes nombradas imagen1.jpg y el archivo imagen2.jpg

imagen1.jpg

imagen 2.jpg

Ilustración 1 y 2 - Colisión MD5

Las imágenes pueden descargarse para corroborar lo mencionado, desde:

https://jocsanlaguna.com/colisionhash

Empleando cualquier herramienta para el cálculo del MD5, se obtiene que ambas imágenes tienen el mismo valor de integridad hash MD5, el cual es: 253dd04e87492e4fc3471de5e776bc3d

Lo cual se corrobora a continuación

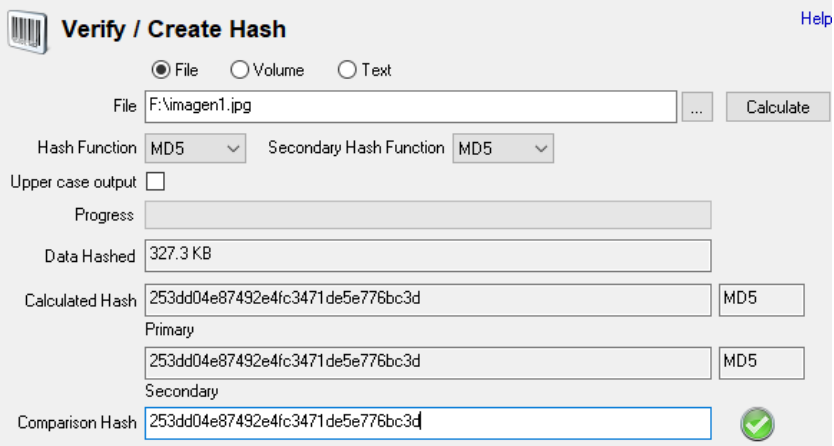


Ilustración 3 - Colisión MD5 demostración

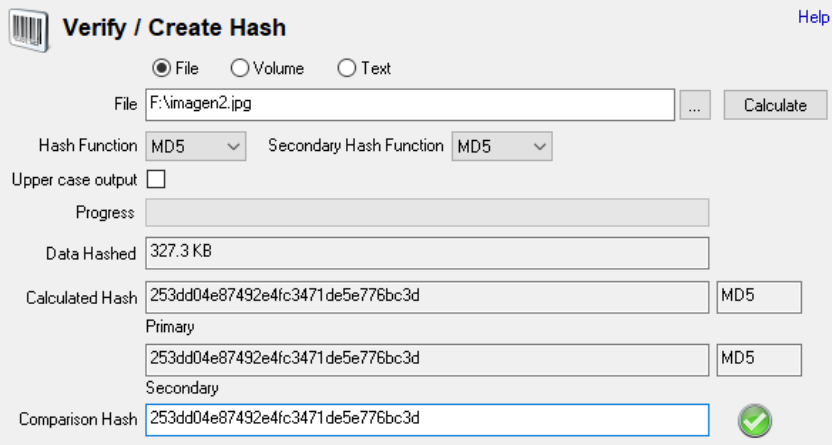
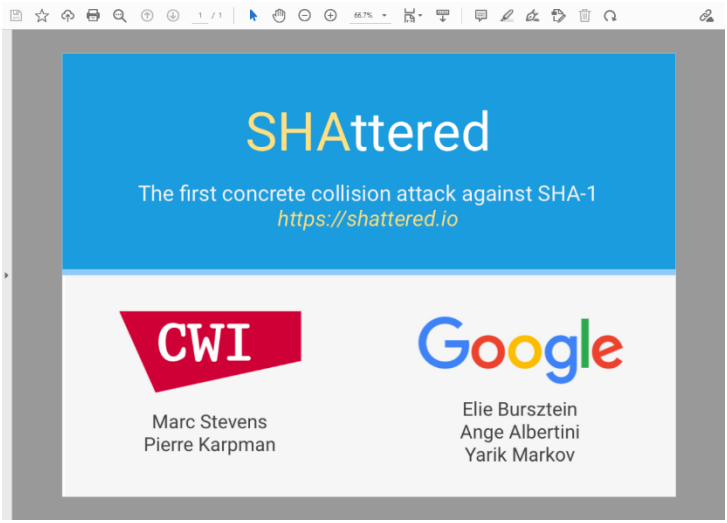


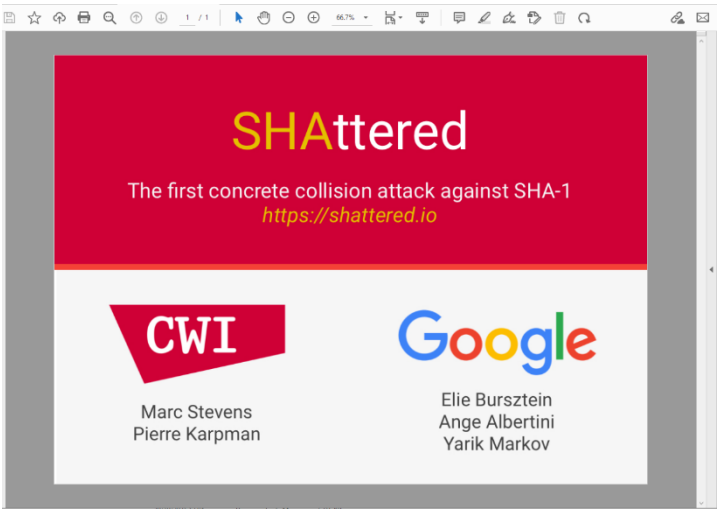
Ilustración 4 - Colisión MD5 demostración

En el ejemplo de las fotos era obvia la diferencia, pero ¿Qué pasaría si es evidencia digital de un homicidio, en donde un video que capturó el rostro del culpable se reemplaza por otro en donde se ve pasar a una persona inocente, o unas bitácoras de operaciones bancarias con cierto número de transacciones son reemplazadas por otras en donde se agrega o eliminan órdenes de pago?

Así como se hizo con el MD5 se puede realizar con el algoritmo SHA-1 una colisión, la cual permite que dos archivos totalmente distintos, posean el mismo valor, lo cual se traduce en la posibilidad técnica de manipular la evidencia que ha sido encontrada.



original.pdf



alterado.pdf

Ilustración 5 y 6 - Colisión SHA1

Llevando a cabo el cálculo del SHA1, podemos observar que ambos archivos pese a ser evidentemente distintos, poseen el mismo valor, por ello, se demuestra que el algoritmo SHA1 tiene una brecha de seguridad que permite que dos archivos digitales distintos, tengan el mismo valor, la cual, para fines prácticos, corrompe toda cadena de custodia y trazabilidad de no alteración que pudiese tener el archivo digital.

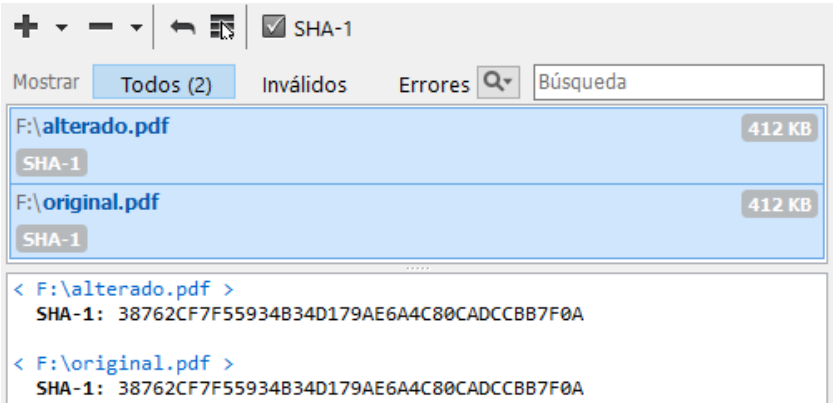


Ilustración 7 - Colisión SHA1 demostración

No existe técnica que nos permita descubrir de un archivo digital (con valor de integridad MD5 o SHA-1), si este ha sido manipulado, es imposible determinar si el elemento digital ha sido alterado o está intacto, por ello, el tema central es que no se puede o mejor dicho, no se debe presentar ante un juez o ante una autoridad elementos con valores de integridad MD5 y SHA-1, por la falta de certeza científica que existe, ambos algoritmos poseen colisiones y

la evidencia digital que se presentó un juicio se podría manipular sin dejar huella.

El algoritmo que da certeza científica hoy, 03 de noviembre del 2021 sería el SHA-256 y también el SHA-512.

El detalle que poseen los algoritmos es el tiempo y los recursos informáticos que se utilizan para su cálculo, a mayor extensión del algoritmo, el tiempo empleado será mayor, un MD5 es por mucho más rápido de calcular que un SHA-1, a su vez el SHA-1 es más rápido de calcular que un SHA-256.

Dentro del tema de preservación, nos enfrentamos también a dudas como ¿si está prendido un equipo de cómputo, lo apago? ¿puedo conectar una memoria USB para extraer evidencia? Por lo que abordaremos los casos principales.

Para preservar la evidencia ¿apagar o no apagar un equipo de cómputo?, creo que esta es la primera pregunta técnica que todos nos hacemos en un inicio y aunque cada escenario se aborda de forma distinta.

Lo recomendado es primero llevar a cabo un volcado de la memoria RAM (Windows o MAC, en Linux no aplica y se explica más adelante), con esto tenemos el registro de la RAM y en nuestro laboratorio podremos analizar, sin embargo, la RAM al apagar el equipo de cómputo se destruye y no existe forma de poder recuperarla, por ello,

es una de las tareas que se hacen de inmediato al llegar a una investigación.

Una pregunta inicial al tener un equipo de cómputo y verlo encendido es ¿cómo apagar un equipo de cómputo? La mejor forma de realizarlo pese a la idea generalizada de muchos, no es dando clic en apagar equipo dentro del propio sistema operativo, no es lo recomendado porque existen muchos programas que pueden realizar tareas de mantenimiento como borrado seguro de todos los archivos temporales, hay programas que se configuran para cuando se apague el equipo de cómputo, sea borrada la papelera de reciclaje y todos aquellos datos que el usuario generó, como no es posible conocer lo que hará el equipo de cómputo al realizar un apagado correcto, lo mejor es tirar de los cables de corriente o si es un equipo laptop, la recomendación sería quitarle la batería o mantener presionado el botón de apagado para realizar un pagado forzoso, el riesgo de daño del disco es prácticamente nulo, los discos mecánicos contienen capacitores cuya función al entrar en una falla de corriente eléctrica, es realizar el expulsado de los elementos mecánicos que pueden dañar la información, en el caso de los discos de estado sólido, no existe cabida a un daño de ese tipo, lo que podría llegar a pasar pero es poco probable, sería un archivo corrupto que no terminó de forma adecuada su escritura, como un archivo de office que se estaba trabajando, más allá de ello los sistemas operativos actuales pueden hacer frente a fallas de corriente.

Esto nos plantea una pregunta que se relaciona con la alteración de evidencia, ¿podemos manipular un equipo de cómputo que es evidencia, es legal ante una autoridad?

La respuesta corta es depende, depende que cambio estamos haciendo, debemos partir del hecho que abrir un programa, cerrar una ventana, conectar una memoria USB genera cambios en el equipo de cómputo, pero esto sí es válido solo si existe una razón de peso de por qué se hace una modificación, por ejemplo, conectar una memoria USB para ejecutar de forma portable un programa y realizar un volcado de la memoria RAM, generó cambios en los registros del equipo, utilizó recursos y claramente alteró la evidencia, sin embargo se justifica dado que la alteración es minúscula, comparado con el hecho de haber extraído la memoria RAM, la cual una vez apagado el equipo de cómputo no es posible recuperar, si lo vemos, el programa portable pudo haber modificados algunos kilobytes, incluso megas, pero obtuvimos 4, 8, 16 o varios Gb de RAM con información valiosa y que se hubiera perdido sin nuestra intervención. Pero con el mismo ejemplo, si en lugar de usar un programa portable decidimos llevarnos un instalador, ejecutarlo en el equipo de cómputo e instalarlo en el propio disco duro de evidencia, ahí la alteración de evidencia difícilmente se justifica, ya que el investigador tenía otros caminos para preservar la evidencia y se fue por uno que escribió sobre el disco duro que es objeto de estudio. Siempre debemos buscar la ruta que menos cambios haga en la evidencia.

1.3 Análisis: Esta categoría comprende casi la totalidad del libro y es el proceso técnico para saber que herramientas debemos usar y como emplearlas para sacarles el mayor provecho, en este apartado solo nombramos el tema, pero en los siguientes capítulos lo desarrollamos.

1.4 Presentación: Nos enfocamos en resumir en un documento lo más relevante de nuestra investigación, al respecto podemos considerar tres tipos de reportes.

- Reporte ejecutivo: Este documento será leído por los directivos de una empresa con un extracto del análisis, pero con énfasis en las conclusiones, no les interesa conocer los valores de integridad hash, ni si usamos una herramienta de código libre o comercial, se busca que en pocas páginas se aporte información concreta y suficiente para la toma de decisiones.
- Reporte técnico: Este acompaña el reporte ejecutivo y está destinado para que el personal de sistemas pueda conocer la metodología y todos esos puntos que son relevantes como el software empleado, los logs analizados y los registros que soportan las conclusiones a las que se llegó.
- Dictamen pericial: Este solo es usado en proceso judiciales, su estructura es una combinación del reporte ejecutivo, pero con el respectivo soporte técnico que sea crucial, solo si aporta algún valor al

caso, se puede dar referencias de que el uso del software o hardware de cómputo forense que se empleó para la investigación, ha sido usado por fuerzas del orden en algún lado o noticias de relevancia para que el juez tenga un escenario más amplio, de igual forma se pueden señalar los elementos técnicos pero muchas veces si son elementos técnicos que el juez no comprendería, pueden ser señalados en el reporte como anexos que acompañan el dictamen pericial, con ello el juez tiene un documento más ligero pero que si quisiera, podría revisar los anexos para entender cómo se llegó a las conclusiones que se plantean en el documento, de igual forma puede ser acompañado con un glosario de términos para que todas esa palabras que una persona de sistemas da por hecho, el juez pueda comprender gracias a su respectiva explicación.

2. Tipos de análisis forenses

Aquí hay diferencias en como clasificar los tipos de análisis, algunos hacen la clasificación a nivel técnico, análisis de redes, análisis de RAM, análisis de equipos de cómputo y la lista podría seguir, sin embargo, considero que existe una clasificación por encima que a su vez engloba la parte técnica y obedece a la pregunta ¿la investigación será con fines legales?

Dependiendo los objetivos que nos presenten, son dos grandes escenarios que engloban a su vez los distintos tipos de investigaciones, investigaciones que no son mutuamente excluyentes.

En el primer grupo están las investigaciones con fines legales, en estas como primer punto debemos saber que habrá derecho de réplica, nuestro reporte será analizado por otro experto y frente a un juez cada investigador defenderá su trabajo, el tratamiento de la evidencia será crucial para salvaguardar la certeza científica de la no alteración de los registros, así como de las herramientas que fueron empleadas para llegar a las conclusiones, si fuera el caso la licencia vigente del software comercial que se haya empleado, toda la actividad del investigador podrá ser revisada y objetada si fuera oportuno.

2.1 La teoría del fruto del árbol envenenado

Es una doctrina que hace referencia a que las pruebas de un delito obtenidas de manera ilícita son per si, ilícitas también, como ejemplo, si se lleva a cabo la intervención no autorizada de un número telefónico, los audios y el contenido de esa grabación sería ilegal en un proceso legal, sin embargo en la informática tenemos un escenario similar, ya que si una de las herramientas que usamos para llevar a cabo nuestra investigación tenía su licencia comercial vencida, resultó en obtención de información sin la autorización del fabricante del software, por ello, el reporte que se pudiese haber generado, resulta irrelevante y sin valor en un juicio.

En un procedimiento legal una estrategia de muchos abogados y peritos en sistemas, y es revisar y con encontrar un solo error en la investigación hecha por la parte contraria, se consigue que esta quede descartada, por ello se debe revisar y cuidad mucho de principio a fin, ya que hasta un error de impresión se toma en cuenta, dentro de estas investigaciones las que se dan con mayor frecuencia y hablo de lo que en Duriva, una empresa líder en México procesa mensualmente es lo siguiente:

- ✓ Correos electrónicos, ya sea para aportarlos como pruebas en un juicio o para demostrar que los correos que aportó la parte contraria carecen de validez.

- ✓ Mensajes por redes sociales, en este grupo podemos hablar de WhatsApp, Telegram, Twitter, Instagram, todas esas redes sociales que nos permiten comunicarnos, pueden ser aportados como pruebas en un juicio, nuestra labor es primeramente extrayendo la información, validando que no haya sido alterado y poniendo a disposición de la autoridad una copia de dichos mensajes.
- ✓ Transferencias bancarias, esto en los últimos años ha incrementado, muchas personas detectan que no han hecho uso de la banca en línea sin embargo su banco señala que todos sus fondos fueron retirados en operaciones a otros bancos, aquí es un tema interesante de llevar una investigación de desvío de recursos.
- ✓ Ubicación de un dispositivo celular, con temas judiciales de índole penal, es requerido que se pueda demostrar la ubicación de un dispositivo celular un día y una hora determinada, para poder demostrar donde se encontraba el dueño del celular cuando en otro lugar posiblemente sucedió un hecho ilícito.

Investigaciones sin fines legales, esto con mayor frecuencia se da en empresas que quieren dar respuesta a dudas planteadas, como el origen de un ataque informático, en muy pequeña medida podemos hablar de personas buscando una investigación, pero podemos categorizarlas en las siguientes:

- ✓ Ataques de ransomware, por lo regular se desea conocer al responsable de que activos de una empresa hayan sido cifrados, esto puede señalar como responsable a un director de sistemas que no aplicó buenas políticas o a un empleado que descargó, utilizó o dio clic en donde no debía y la empresa resultó con un cifrado.
- ✓ Ataques a sitios de internet, podemos verlo con empresas o escuelas cuyo portal de internet fue atacado y derivó en una fuga de información, muchas veces el objetivo solicitado es encontrar cómo fue posible el ataque, porque de antemano se sabe que quien estuvo detrás de dicha irrupción informática, uso conexiones VPN que dificultan su rastreo.
- ✓ Infidelidades, aquí en definitiva son particulares quienes llegan a requerir el análisis de un dispositivo celular que en muchas ocasiones está incluso bloqueado, solicitando que se recuperen mensajes de redes sociales, fotos y videos eliminados.

3. Recolección de evidencia

Cuando somos convocados a una investigación y llegamos a sitio, es recomendado llevar un formato que nos permita llenar los aspectos más importantes de la investigación ya que podríamos pasar por alto aspectos importantes.

Al llegar a una investigación mi recomendación personal es fotografiar el lugar y los equipos de cómputo, para prevenir que, si un equipo tenía un golpe o un daño, este se nos pueda atribuir a nosotros, de igual forma recomiendo tomar los datos generales de quién fue el que nos puso a la vista los equipos de cómputo, la hora en que tuvimos a la vista el equipo informático, así como la hora que mostraba dicho equipo informático.

Otra recomendación importante, es escuchar al personal de sistemas, pero desconfiar de ellos, si fuera el caso que un ataque informático se haya producido por un mal manejo de políticas de seguridad, instalación de parches, actualización del antivirus, la responsabilidad del equipo de sistemas se vería afectado, por ello es recomendado guiarnos por nuestras prácticas y técnicas, no así por sugerencias o aportaciones de los departamentos internos de una empresa.

3.1 Antes de iniciar

Debemos tener siempre listas las herramientas, discos y demás elementos de los que haremos uso en una investigación, algunos puntos requieren un poco de tiempo para estar preparados, por eso es importante dedicar tiempo a este punto.

Discos duros y memorias USB.- Al realizar una copia forense, esta será almacenada en un medio de almacenamiento externo, por lo regular es un disco duro, el cual deberá haber sido formateado previamente con un formateo lento, el cual sobrescribe todos los sectores del disco con valores de 0 a nivel binario, esto es fundamental, ya que si el disco que soporta la copia forense contiene información, archivos, videos o cualquier elemento de un caso previo, tendríamos una mezcla de información la cual nos dañaría por completo nuestra cadena de custodia, siempre debemos formatear con una, dos o hasta tres formateos lentos para tener la tranquilidad y confianza que nuestro disco duro que llevamos a sitio está limpio.

Herramientas forenses portables.- Como ya lo mencionamos anteriormente, debemos evitar instalar lo que fuera en el equipo de cómputo que vamos a investigar, por esa razón debemos tener a la mano las herramientas portables que usaremos en el caso al que nos llamen, pero debemos prevenir diversos escenarios, como el que algunas aplicaciones forenses hacen uso de algunos

Frameworks de Windows, que de no estar en el equipo, no se podría ejecutar nuestra herramienta forense, debemos contar con una, dos o hasta tres alternativas para cualquier tarea que queramos hacer.

Binario estáticos. – Es ampliamente recomendado, que llevamos siempre nuestra CMD portable, es peligroso ejecutar cualquier instrucción dentro de la línea de comandos de un equipo de cómputo que vayamos a analizar, ya que es posible que alguien haya hecho una modificación y un simple comando “dir”, realice una acción de borrado o apagado del equipo de cómputo, es algo que debemos prevenir y por ello todo lo que ejecutemos debe correr en nuestro kit de herramientas portable.

3.2 Diferencias entre copia forense y backup

La idea generalizada de backup es muy común hoy en día, lo vemos cuando cambiamos de dispositivo celular y queremos conservar nuestros contactos, fotos y demás archivos, sin embargo en la informática forense este concepto o lo que representa, tiene poco valor, la labor de un investigador forense digital se encamina a generar una copia completa del medio origen, esto incluye lo que vemos como espacio en blanco dentro de una unidad, este “espacio disponible”, en realidad contiene todos los archivos que fueron eliminados, por ello resulta crucial en una investigación, nos resulta clave al momento de realizar

el análisis de archivos borrados así como en su recuperación.

El espacio disponible, también se conoce como espacio vacío y en los programas informáticos que veremos, se le nombra como “unallocated space”.

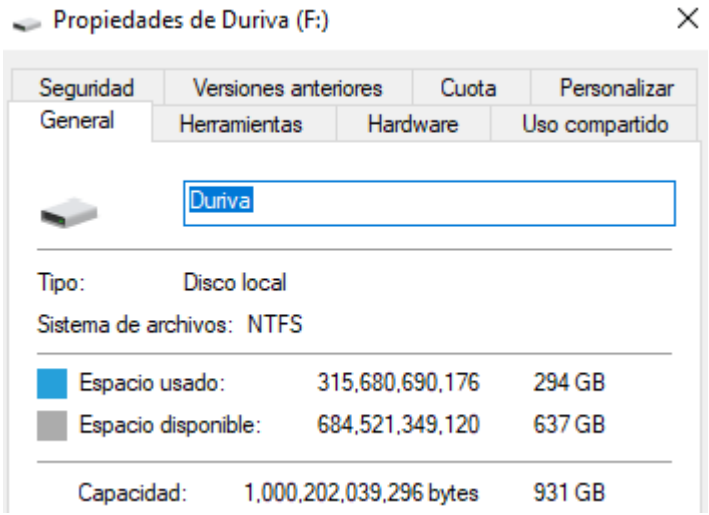


Ilustración 8 - Diferencias backup y copia forense

Un backup de la unidad mostrada en el gráfico anterior, tendría un tamaño de 294 Gb, sin embargo, una copia forense, tendría un tamaño de 931 Gb, ya que el “espacio vacío” se copia tal y como está en el medio origen, con todos aquellos datos que pudieran existir. (es posible generar backups y copias forenses con factores de compresión, lo cual solo reduce el tamaño de la copia, sin

afectar la integridad de la copia yo se sigue aplicando la misma diferencia de concepto)

3.3.1 Memoria RAM en sistemas Windows

Al hablar de los primeros pasos que se realizan cuando llegamos a sito y nos damos cuenta de que los equipos de cómputo objeto de estudio se encuentran encendidos, habíamos señalado ya que la memoria RAM será crucial, por ello debemos proceder a la extracción de esta.

Existen herramientas gratuitas y comerciales que nos permiten obtener la copia de la memoria RAM, también conocido el proceso como volcado de memoria, es indistinto el uso de las herramientas a nivel técnico ya que todas consiguen una copia de la memoria RAM, el cambio se presenta en la interfaz gráfica que en algunos casos es más o menos intuitiva, y con más o menos opciones por configurar, de las principales herramientas podemos encontrar a:

- FTK Imager[1]
- OSForensic[2]
- Belkasoft Live RAM Capturer[3]

[1] https://accessdata.com/product-download/
[2] https://www.osforensics.com/download.html
[3] https://belkasoft.com/ram-capturer

Veamos un ejemplo de captura de memoria, en este caso usaremos FTK Imager, una vez ejecutado el programa, tendremos una interfaz gráfica que contiene un botón el cual dice “Capture Memory”

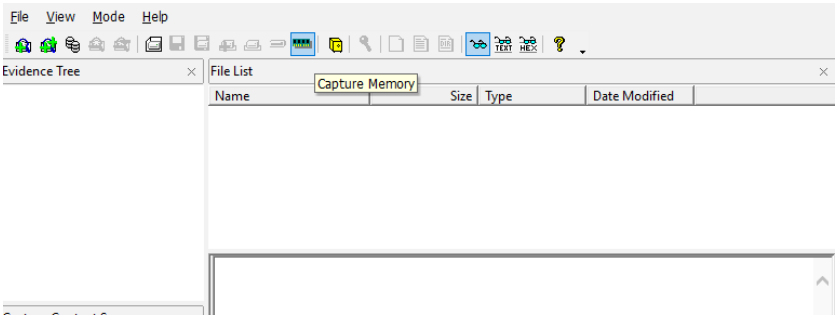


Ilustración 9 - Copia de la memoria RAM con FTK

Este botón al darle clic nos abrirá una ventana la cual nos solicita que definamos la ruta de destino y el nombre que le asignaremos el archivo del volcado de memoria.

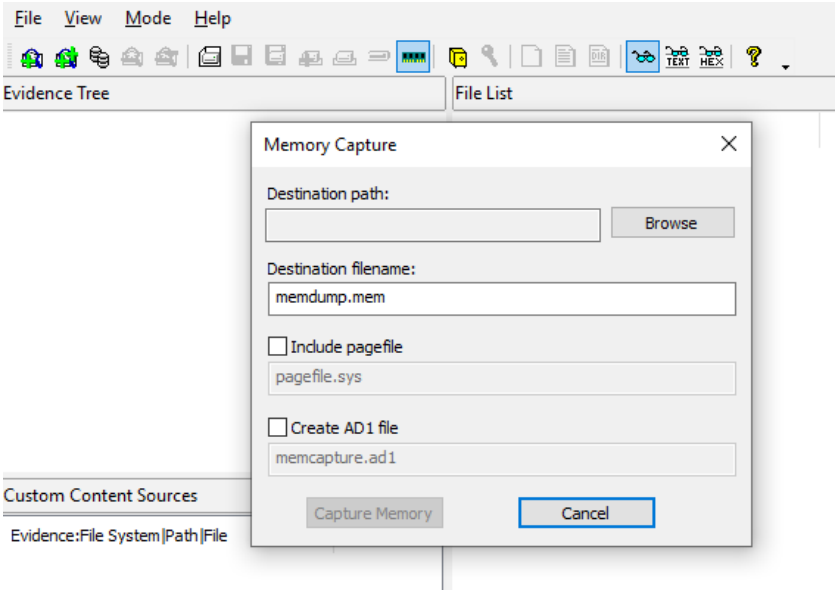


Ilustración 10 - Copia de la memoria RAM con FTK

Con pasos más o menos, este sería en términos generales el proceso en las demás herramientas de cómputo forense, probando la herramienta “Belkasoft Live RAM Capturer”, en algunas uno puede habilitar o deshabilitar que, al realizar la copia de la memoria, sea considerado el archivo de paginación (extensión de la memoria RAM que se almacena en el disco duro).

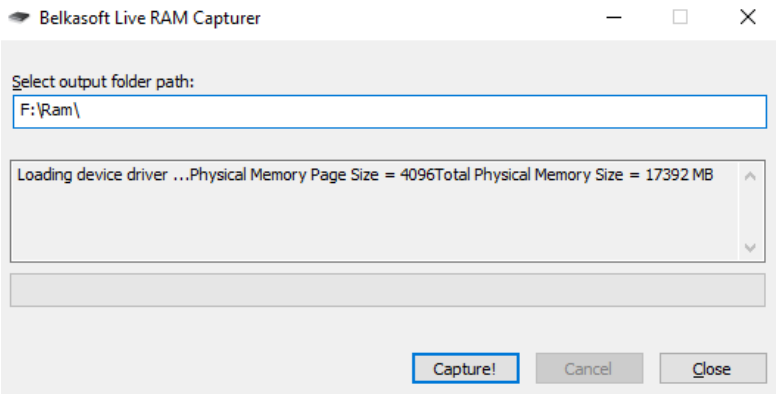


Ilustración 11 - Copia de la memoria RAM con Live RAM Capturer

El siguiente paso sería llevar a cabo la obtención del valor de integridad hash, del cual ya hemos hablado, por lo que una herramienta portable podría ser Multihasher, con dicha herramienta podemos seleccionar el algoritmo que nos interesa emplear y la ruta del archivo, para que el programa nos entregue como resultado, la cadena de texto del valor hash requerido.

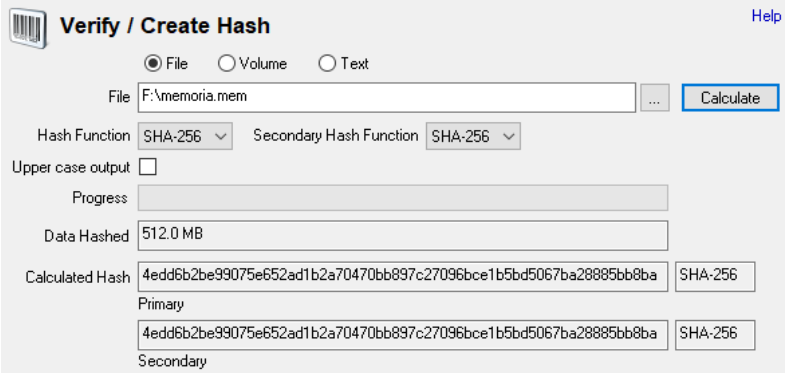


Ilustración 12 - Copia de la memoria RAM con Live RAM Capturer

Dentro de la memoria RAM, debemos conocer que hay dos lugares de los cuales podemos mandar a llamar información, la primera es la propia información guardada en la memoria RAM físicamente, por otro lado, los sistemas operativos Windows, hacen uso de una fracción del disco duro para guardar una extensión de la memoria, la cual se conoce como paginación.

Aunque un método alternativo para acceder a la memoria RAM sería generar un error en el sistema (la famosa pantalla azul), esta es poco sugerida ya que se genera una copia parcial o integra de la memoria RAM dentro del disco duro, como hemos platicado, siempre debemos procurar hacer el menor impacto en la modificación de a evidencia, razón por la cual desaconsejo usar ese método en la medida de lo posible.

3.3.2 Memoria RAM en Linux

En los sistemas Linux tenemos la ventaja de no requerir programas externos, la propia línea de comandos del sistema será nuestra herramienta forense, para ello, existe un comando llamado “dd”, el cual encontraremos en cualquier versión de Linux e incluso en los sistemas MAC, este comando es el que nos va a permitir realizar una copia de un origen a un destino incluyendo el “espacio vacío” que vimos anteriormente.

El comando tiene una sintaxis muy simple y a la vez potente.

Ilustración 13 - Copia en Linux con dd

En la imagen anterior estamos realizando la copia de la ruta /dev/sdb y la estamos arrojando en la carpeta escritorio.

Sabiendo que la ruta de la memoria RAM en Linux está ubicada en /dev/mem este comando dd era suficiente para realizar la copia de la RAM, sin embargo, a partir del Kernel de Linux 2.4.x, ya no es posible, esto no es posible ni con permisos de super administrador, ya no podemos acceder

a la memoria RAM de forma directa, ya que el fichero “mem”, no le pertenece el usuario super administrador, sino al Kernel, por ello al intentar realizar una copia, el sistema arroja un error y genera un log del intento de acceso a este fichero.

```
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
forense@Tequila:~$ sudo dd if=/dev/mem of=/home/forense/Escritorio/ram.dd
[sudo] password for forense:
dd: error al leer '/dev/mem': Operación no permitida
2048+0 registros leídos
2048+0 registros escritos
1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.013624 s, 77.0 MB/s
forense@Tequila:~$
```

Ilustración 14 - Copia en Linux de la memoria RAM con dd

Si bien, existen herramientas como LiME que pueden ayudarnos a realizar una copia de la memoria RAM en Linux, esto es algo delicado, ya que son cambios hechos el sistema operativo que se graban en disco, no es una modificación menor la que estamos haciendo y defender esta serie de modificaciones frente a una autoridad sería una labor complicada.

Pero no todo está perdido con respecto a los elementos que están en RAM, dentro de la unidad, existe una carpeta que conserva información detallada de cada uno de los procesos, la carpeta es /proc

ls .- el comando nos permite conocer el contenido de archivos dentro de un directorio

ps.- este comando muestra los procesos que se encuentran en ejecución, el comando puede llevar variantes adicionales como ps aux, ps axjf, sin embargo se deja al lector la recomendación de investigar los principales comandos en Linux.

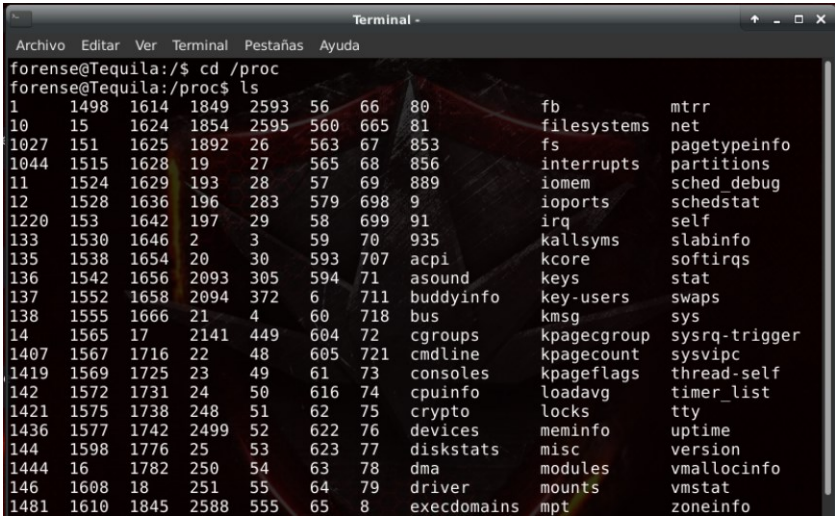
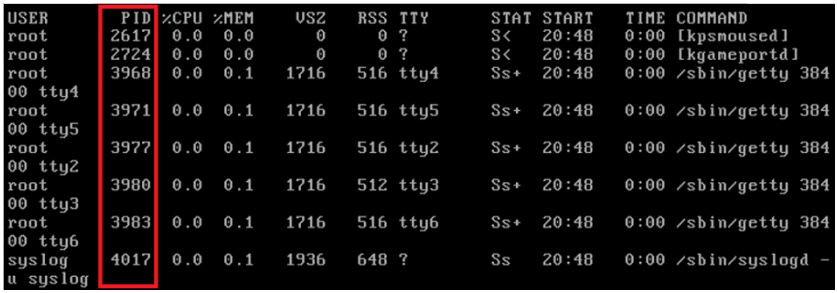


Ilustración 15 – Acceso a procesos /proc en Linux

Al dar un “ls” dentro de /proc podemos encontrar que existen diversos directorios y muchos de ellos su nombre es un número, esto lo podemos comprender aún mejor si dentro del equipo ejecutmos “ps” con alguna de sus variantes, como “ps aux”



```
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root       2617  0.0  0.0      0     0 ?        S<   20:48   0:00 [kpsmoused]
root       2724  0.0  0.0      0     0 ?        S<   20:48   0:00 [kgameportd]
root       3968  0.0  0.1   1716   516 tty4     Ss+  20:48   0:00 /sbin/getty 384
00 tty4
root       3971  0.0  0.1   1716   516 tty5     Ss+  20:48   0:00 /sbin/getty 384
00 tty5
root       3977  0.0  0.1   1716   516 tty2     Ss+  20:48   0:00 /sbin/getty 384
00 tty2
root       3980  0.0  0.1   1716   512 tty3     Ss+  20:48   0:00 /sbin/getty 384
00 tty3
root       3983  0.0  0.1   1716   516 tty6     Ss+  20:48   0:00 /sbin/getty 384
00 tty6
syslog     4017  0.0  0.1   1936   648 ?        Ss   20:48   0:00 /sbin/syslogd -
u syslog
```

Ilustración 16 – Listado de procesos en Linux

La segunda columna nombrada “PID”, refleja el número de identificación del proceso listado, el cual, podremos encontrar detallado en la carpeta /proc, esto nos permite entender que la carpeta “proc” tendrá mucha información valiosa de los procesos y será una fuente de información muy importante, que, si bien la memoria RAM estaba protegida y no permitía su copiado de forma directa, podemos irnos con los datos de proc.

De igual forma que Windows hace uso de una parte del disco duro como una extensión de la memoria RAM, en Linux encontramos una partición de disco destinada a ello, se conoce como SWAP y si bien podemos copiarla, el estar dentro del disco duro como una partición, no sería indispensable que se copie cuando el equipo está encendido.

3.4 Comandos de Windows como herramientas forenses

Ya hemos platicado que debemos llevar nuestra propia CMD portable, por ello haciendo uso de comandos propios de Windows, es posible extraer una gran cantidad de información, el siguiente es el listado por orden alfabético de algunas de las herramientas que podemos consultar.

Comando	Descripción
arp	Muestra tablas de Protocolo ARP.
date	Muestra la configuración de fecha actual.
doskey	Muestra el historial de comandos para CMD.EXE.
ipconfig	Muestra la configuración local del equipo.
netstat	Muestra la información de conexión actual.
time	Muestra la configuración de hora actual.
schtasks	Muestra las tareas programadas.

systeminfo	Proporciona información general acerca del equipo.
hostname	Muestra el nombre de host del equipo.

Ilustración 17 – Comandos de Windows aplicados a forense

3.4.1 Tablas de protocolo ARP

De forma temporal, se crea un listado en cada una de las interfaces de red con una relación entre las direcciones ip y las direcciones físicas registradas, esta tabla es importante ya que podemos conocer si es de un tipo estático o fue creado de forma manual.

```
H:\>arp -gv

Interfaz: 127.0.0.1 --- 0x1
  Dirección de Internet          Dirección física      Tipo
  224.0.0.2                                            estático
  224.0.0.7                                            estático
  224.0.0.22                                           estático
  224.0.0.251                                          estático
  224.0.0.252                                          estático
  239.255.255.250                                      estático

Interfaz: 192.168.127.1 --- 0x7
  Dirección de Internet          Dirección física      Tipo
  192.168.127.2                 [redacted]-00-00      no válido
  192.168.127.254               [redacted]-22-8f      dinámico
  192.168.127.255               [redacted]-ff-ff      estático
  224.0.0.2                     [redacted]-00-02      estático
  224.0.0.7                     [redacted]-00-07      estático
  224.0.0.22                    [redacted]-00-16      estático
  224.0.0.251                   [redacted]-00-fb      estático
  224.0.0.252                   [redacted]-00-fc      estático
  239.255.255.250               [redacted]-ff-fa      estático
  255.255.255.255               [redacted]-ff-ff      estático
```

Ilustración 18 – Protocolo ARP

3.4.2 Historial de CMD

En este punto tenemos un debate, ya que el comando doskey /history nos muestra el historial de comandos colocados en CMD, sin embargo, de usarlo en nuestra CMD portable nos mostraría el historial de los comandos que como investigadores pusimos, lo ideal sería ejecutarlo desde la máquina que estamos analizando, sin embargo, no podríamos estar tranquilos de ejecutarlo sin saber qué hará la aplicación.

```
H:\>doskey /history
netstat -abonp
netstat -abon
netstat -abo
netstat -an
arp -h
arp -gv
doskey
doskey -h
doskey /history
```

Ilustración 19 – Historial de CMD

3.4.3 Configuración de red en Windows

En una primera instancia la configuración de red nos puede parecer trivial, sin embargo, es importante conocer como es que el equipo de cómputo que tenemos enfrente interactúa en la red de área local, en el caso de servidores, notaremos que tienen más de una salida de red, para poder dar servicios y proporcionar acceso a documentos de la empresa, por más de una vía, en el caso de que una red falle, se tenga otra independiente que permita continuar con las operaciones dentro de un corporativo.

Haciendo uso del comando “ipconfig /all”, se nos desplegará un listado con la distribución de red que se tenga, incluyendo la configuración de redes VPN o si fuera el caso, el detalle de cada uno de los adaptadores de red con los que cuente el equipo, además de la dirección IP asignada a cada uno de los adaptadores.

Ilustración 20 – Configuración de red

3.4.4 Conexiones activas en Windows

Mediante el uso del comando “netstat” podemos conocer las conexiones de red activas e interactuando con las opciones de este comando, ordenar el resultado por protocolo, señalando la dirección remota a la que se ha establecido una conexión o se mantiene un estado de escucha.

```
H:\>netstat -an

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
```

Ilustración 21 – Conexiones de red activas

Dentro de las herramientas gratuitas, una bastante interesante que realiza la misma acción que netstat, es “currports” [4], la ventaja de esta herramienta es la interfaz gráfica que nos permite interactuar en un ambiente visual así como con la exportación de los resultados a distintos formatos.

[4] https://www.nirsoft.net/utils/cports.html#DownloadLinks

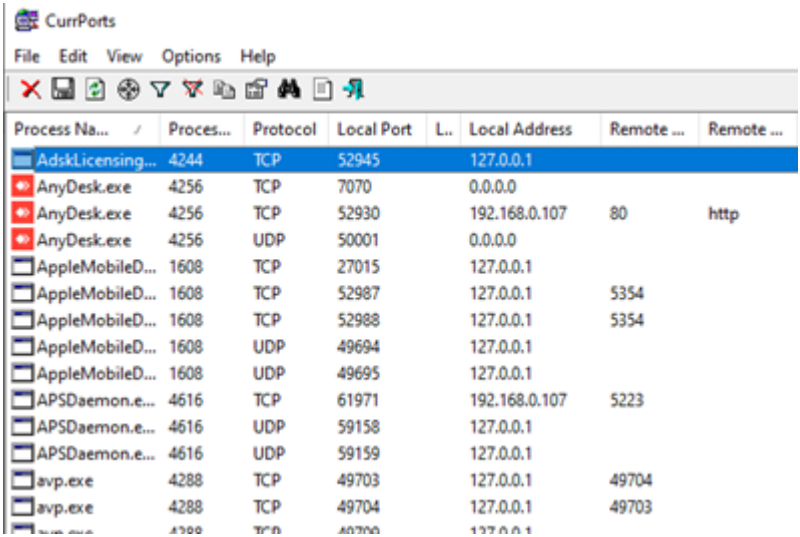


Ilustración 22 - CurrPorts

3.4.5 Tareas programadas

Con este comando podemos conocer las tareas programadas, la próxima hora de ejecución, así como la ruta en donde se ejecuta la tarea.

```
H:\>schtasks

Carpeta: \
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== =======
Adobe Acrobat Update Task                08/11/2021 10:00:00 p. Listo
AdobeGCInvoker-1.0                       09/11/2021 08:55:00 a. Listo
GoogleUpdateTaskMachineCore              09/11/2021 04:10:17 p. Listo
GoogleUpdateTaskMachineUA                08/11/2021 08:10:17 p. Listo
iSCSIAgentAutoStartup                    N/A                    Listo
MicrosoftEdgeUpdateTaskMachineCore       09/11/2021 11:29:48 a. Listo
MicrosoftEdgeUpdateTaskMachineUA         08/11/2021 07:59:48 p. Listo
```
Ilustración 23 - Tareas programadas

3.4.6 Información del sistema

De los comandos que demoran más tiempo en su ejecución es “systeminfo”, son un par de instantes en lo que recaba un detallado reporte del equipo de cómputo, entre ellos versión del sistema operativo, compilación, muy importante la fecha del de instalación del sistema operativo, tipo de placa base, configuración del sistema, tipo de arquitectura, detalle del uso de la memoria RAM, ubicación del archivo de paginación y detalle de actualizaciones aplicadas.

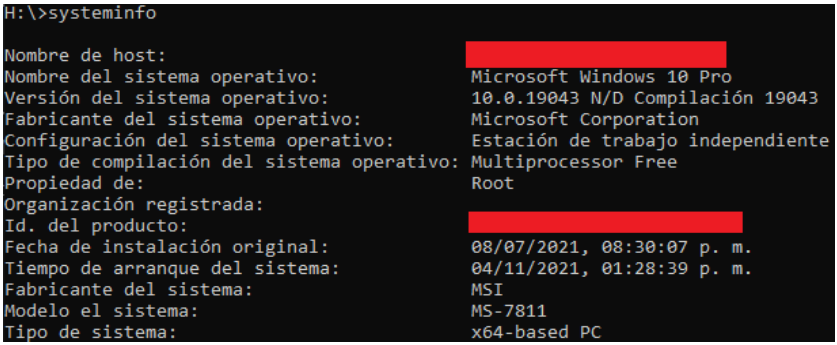


Ilustración 24 - Información del sistema

3.5 Historial de navegadores

Aunque es posible llevar a cabo el análisis de la actividad en los principales navegadores web, mi recomendación es no hacerlo con el equipo de cómputo encendido, ya que herramientas portables existen varias, sin embargo, salta a escena un factor importante y es que el archivo que está

asociado con el historial de navegación tiene en sus propiedades la fecha de última apertura, herramientas que nos permiten visualizar el historial de actividad no son esencialmente necesarias de ejecutarse de forma portable, lo ideal es que hagamos uso de ellas en nuestro laboratorio, ya que la copia forense fue generada y no corremos el riesgo de alterar la trazabilidad de la evidencia.

De entre las herramientas que nos permiten generar un listado del historial de navegación destacan

- **MozillaHistoryView**
- **ChromeHistoryView**
- **IEHistoryView**

Si en nuestro laboratorio decidimos hacer uso de ellas, es posible generar una maquina virtual con el disco de la copia forense, con ello podremos hacer uso de las herramientas como estas de las cuales es muy simple su uso y aportan muchos datos, lo único que requerimos es ejecutarlas en la sesión del usuario del que nos interesa analizar su actividad, ya que no realizan un reporte multi usuario.

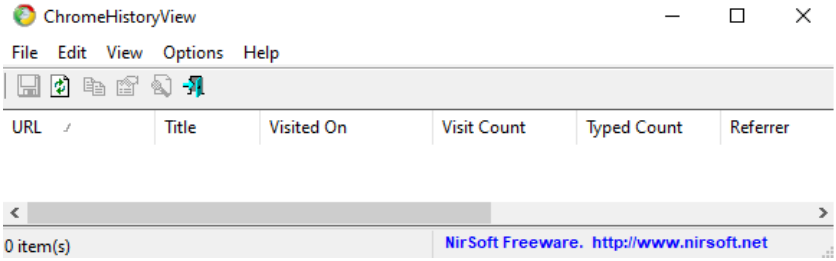


Ilustración 25 – Historial de navegación en Chrome

El aspecto que más destaca al usar estas herramientas es exportar los resultados, la recomendación que se debe recordar es exportar siempre a “csv”, ya que los datos con este formato nos permiten trabajar posteriormente abrir el fichero con un editor de hojas de cálculo como Excel y aplicar filtros dentro de filas y columnas.

3.6 Utilidades

Existen herramientas que nos simplifican el trabajo en cuanto a la obtención de elementos en sistemas encendidos, si bien podemos preparar previamente una memoria USB con estas utilidades, ya hay gente que se ha dado a la tarea de ello y veremos que con solo un par de clic podremos extraer mucha información general

La duda que seguramente muchos tendrán, es, ¿Por qué obtener la información en este momento y no ya en nuestro laboratorio trabajando sobre la copia forense?, la respuesta es muy simple y es eso, si extraemos esta información es

invertir un par de minutos para llevarnos los reportes y en nuestra laboratorio analizarlos, lo cual nos ahorra una gran cantidad de horas y en varios casos, podríamos tener la respuesta a la investigación sin tener que realizar un proceso exhaustivo de investigación sobre la copia forense.

3.6.1 Agave

Esta utilidad fue desarrollada por el autor del presente libro, en mi paso por la universidad y se liberó en 2015 por medio de la Universidad UNAM, contiene una gran cantidad de herramientas clasificadas de acuerdo con su uso.

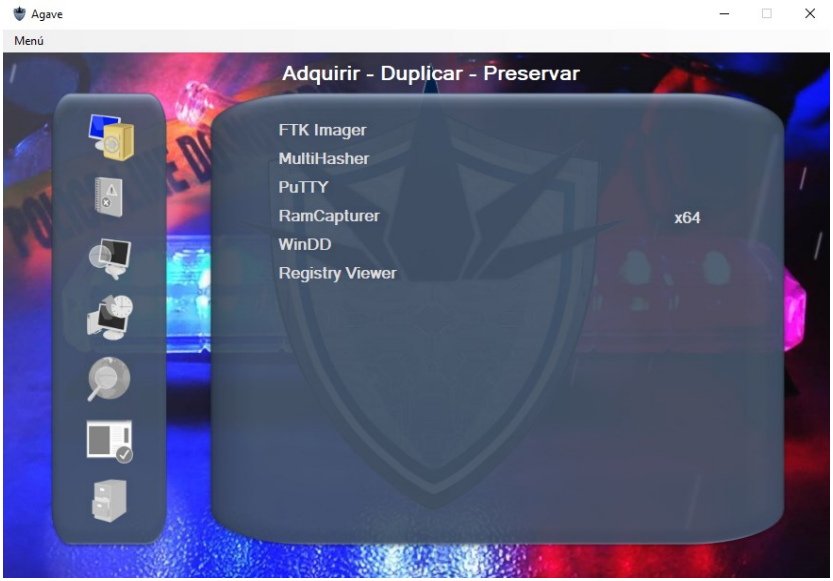


Ilustración 26 – Agave Forense

Las herramientas del lado izquierdo tienen su clasificación:

- Adquirir – Duplicar Preservar
- Analizar Bitácoras
- Reconocimiento del sistema
- Recuperar
- Redes
- Suite
- Utilidades

Agave permite lanzar una a una las aplicaciones para que el usuario elija que desea visualizar y el exportado de los resultados se deja a discreción del investigador.

Se pude descargar desde: https://tequila-so.org

3.6.2 WinTriage

Esta herramienta fue desarrollada por un gran amigo mío, experto con una sorprendente trayectoria en el sector, Lorenzo Martínez, desde la empresa Securízame.

Una nota sobre esta aplicación es que una vez descargada, aun debemos colocarle en sus respectivas carpetas las aplicaciones que por temas de licencia no podían estar en la propia aplicación y entregársele de forma directa a los investigadores. Sin embargo, el proceso de adicionar los

programas necesarios no demora más allá de 5 minutos, por lo que es una muy buena opción.

Ilustración 27 - WinTriage

Una ventaja muy importante es que el investigador puede seleccionar sus objetivos de extracción y la herramienta realiza el proceso de forma automática.

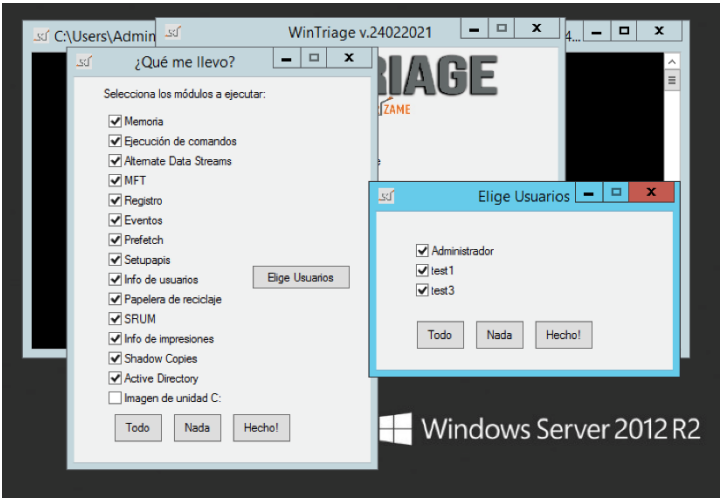


Ilustración 28 – WinTriage opciones

WinTriage se puede descargar desde: https://www.securizame.com/wintriage-la-herramienta-de-triage-para-el-dfirer-en-windows/

3.6.3 WinUFO

Impulsada por los desarrolladores de Caine, esta herramienta aunque fue descontinuada, en funcionamiento es muy similar a Agave, ya que contiene las herramientas ordenadas de acuerdo con los objetivos y el investigador decide que aplicación desea lanzar.

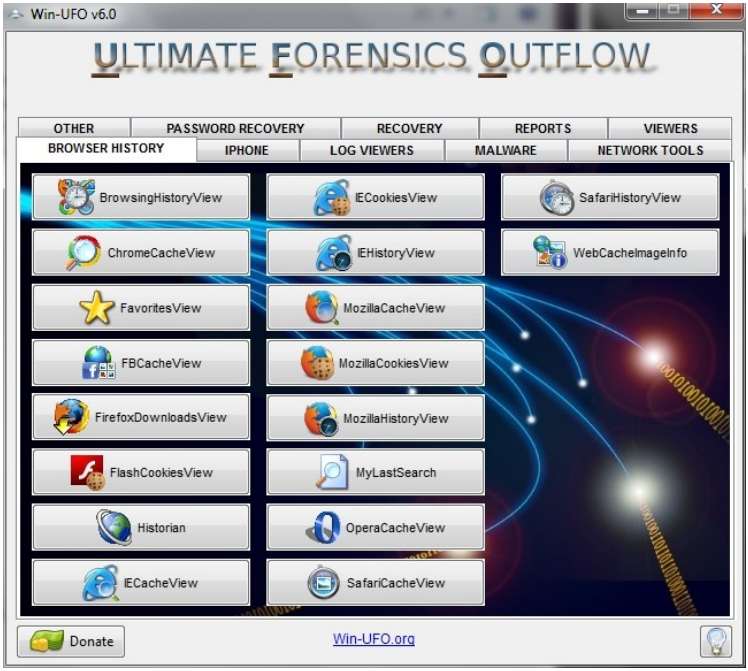


Ilustración 29- WinUFO

4. Copia forense

Como ya hemos hablado en capítulos previos, las investigaciones de informática forenses están focalizadas en poder tener una copia integra del dispositivo de cómputo sobre el cual se llevará a cabo el análisis (o lo más cercano que las posibilidades lo permitan), para poder trabajar sobre dicha copia y no comprometer en nuestros procesos de análisis la evidencia digital original, por ello la copia forense resulta fundamental dentro del área.

4.1 Tipos de copias forenses

De acuerdo con el objetivo que tengamos, de un disco duro podemos llevar a cabo una copia con resultados muy distintos, todas las herramientas forenses te permiten seleccionar uno de los siguientes objetivos por lo cual es menester su conocimiento.

- Físico: Esta copia es la más completa de todas, de un disco duro de 1 Tb se tiene como resultado una copia exactamente 1 Tb (en formatos podemos comprimir el resultado, pero esto es un subtema), dentro de esta copia están todas las particiones que tiene especificado el disco duro, así como el espacio vacío, con ello se tiene una copia integra a nivel físico del disco y además da la posibilidad de

recuperar archivos que fueron eliminados del disco origen.

- Lógico: Aquí debemos seleccionar de un medio de almacenamiento, solo la partición sobre la cual se realizará la copia forense, solo estaríamos copiando los archivos existentes, sería a nivel práctico muy similar a una copia de seguridad de una partición.
- Específico: En este caso solo llevaríamos a cabo la copia de carpetas o archivos específicos, esto es muy usado cuando por ejemplo queremos copiar la bandeja de correo de un usuario, sin embargo, la legislación no nos permite llevarnos más datos de los intrínsecamente necesarios.

4.2 Formatos de copias forenses

Existen distintos formatos con los cuales realizar una copia, todos ellos cumplen con el objetivo de tener como resultado una copia integra del elemento origen, las diferencias entre cada uno de los formatos gira en torno a la compresión, rapidez de la copia, pero más importante podría decirlo, con la compatibilidad que se tendrá posteriormente con las herramientas que en nuestro laboratorio usaremos.

- dd: Este es el formato más básico pero universal para realizar una copia forense, se realiza byte por byte y el resultado puede ser uno o múltiples archivos, en este formato no tenemos la opción de compresión por lo que el resultado será un archivo

con el mismo tamaño que el medio origen, este formato es comúnmente llamado formato en bruto o RAW. Un punto importante de este formato es que toda la información relativa a la copia como software empleado, hardware y valores de integridad hash no están en el archivo de copia, por lo regular las herramientas generan un archivo txt con dichos detalles o manualmente uno debe crearlo. La mayor ventaja que tiene el formato dd es la compatibilidad, todas las herramientas gratuitas y comerciales del mercado, pueden trabajar con copias dd, por ello la compatibilidad está garantizada.

- E01: Este formato fue desarrollado por la empresa EnCase, el formato recibe el nombre de EnCase Evidence Format, podemos decir que es una evolución del formato dd, con las mejoras de que dentro del propio archivo de la copia forense, se incluye la información de las notas del examinador, valor hash MD5, factor de compresión y cifrado. Resulta ser un formato muy atractivo por las ventajas que ofrece, en cuanto a compatibilidad la mayoría por no decir casi todas las herramientas forenses gratuitas son compatibles, en cuanto a herramientas comerciales la compatibilidad está garantizada. El detalle con este formato es que al ser desarrollado por una empresa y no ser abierto, no existe documentación de este, sin embargo, ha

sido muy aceptado por la comunidad y es ampliamente usado.

- AFF: En lo que respecta a este formato llamado Advanced Forensics Format, podemos decir que es un formato abierto que incorpora la compresión y el cifrado de la copia, en cuanto a su compatibilidad las herramientas forenses gratuitas más importantes son compatibles, en cuanto a las comerciales no se tiene una completa compatibilidad.
- Smart: Este formato tiene sus orígenes como una utilidad en Linux para trabajar con particiones de disco, el uso y la compatibilidad de este formato sería a día de hoy algo limitado.

Existen además formatos privados de herramientas comerciales, no abordamos dichos formatos ya que su uso no es general y son exclusivos para el uso de una sola herramienta propia del desarrollador.

4.3 Principales retos

¿Es un disco SATA, SAS, PCIE, USB, SCSI? ¿pero de qué medida es? Este es uno de los mayores retos que nos enfrentamos a llegar a sitio y disponernos de realizar una copia forense, ya que en muchas ocasiones somos llamados de emergencia y no nos informan las

características de los discos, lo recomendado es tener conectores para todos los discos.

Cada vez que vemos un disco debemos pensar si es que tenemos el conector específico que se debe emplear y además dimensionar la cantidad de tiempo que nos llevará realizar el proceso completo.

Demos un repaso, no de la historia y los datos que fácilmente podríamos encontrar en la Wikipedia de los discos, sino un repaso con fines forenses de los principales tipos de disco.

SATA: Es uno de los formatos mas usados, prácticamente la totalidad de los equipos de escritorio y laptops los emplean (excepto dispositivos Apple recientes), por lo que sería muy recomendado contar con este conector por la alta demanda de uso que se tiene, es importante señalar que existen distintas versiones, SATA I, SATA II y SATA III, dependiendo el tipo de conector se manejan distintas velocidades en papel que manejan cada uno de los discos, en la práctica podemos decir que una copia de un SATA I tendrá una velocidad promedio de 22 Mb/s, SATA II alcanza en promedio 60 Mb/s y SATA III en discos duros mecánicos hasta 120 Mb/s en discos de estado sólido en mi práctica he alcanzado hasta 195 Mb/s sostenidos (constantes).

SAS: Es al día de hoy el tipo de disco más común en servidores, comparte con SATA hasta cierta compatibilidad, ya que si los miramos, son muy similares, tal así que físicamente podemos conectar lo discos SATA a cables SAS y viceversa, SIN EMBARGO, esto no quiere decir que vamos a poder leer los discos, los discos SAS requieren una tarjeta controladora para su lectura, esto se traduce en que es necesario un dispositivo específico para poder leer los discos, por ello, desde ya advierto a los lectores, que no existen adaptadores de SAS a SATA. En cuanto a velocidades de copia, estamos hablando de un promedio base de 320 Mb/s sostenidos para discos duros mecánicos, los discos SSD pueden superar estas velocidades.

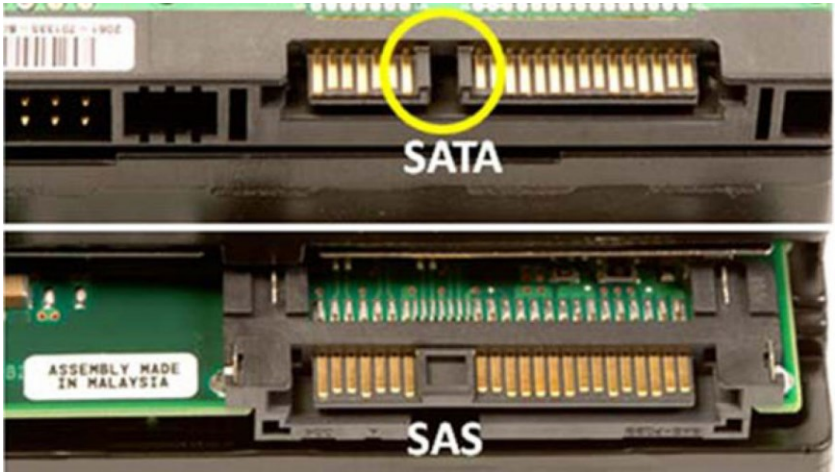


Ilustración 30 – Discos SATA vs SAS

SCSI: Orientados para servidores, los discos duros SCSI por su antigüedad están casi en desuso, sin embargo, por su antigüedad es casi imposible verlos en servidores que dan servicios a usuarios finales, más bien los podríamos encontrar en sistemas industriales que fueron adquiridos hace muchos años. Estos discos tienen la característica principal en que existen varias versiones de SCSI, haciendo aún más difícil nuestra tarea de tener una compatibilidad con todo tipo de disco.

Ilustración 31 – Discos SCSI

USB: Los discos duros que se conectan por medio de USB, en su mayoría internamente son discos duros SATA con un adaptador a USB, la velocidad de estos discos en promedio ronda los 120 Mb/s

Ilustración 32 – Discos duros USB

PCIE: Estos discos ya tienen años ene el mercado, su uso masivo se dio por medio de Apple, que los incorporó en sus laptops y equipos de escritorio, las tazas de transferencia de una copia rondan los 1,100 Mb/s

Ilustración 33 - Discos duros PCIE (modelo Aorus AIC PCIE)

M.2: Estos discos los podemos encontrar con mayor frecuencia en equipos de escritorio ya que requieren que la tarjeta madre cuente con una ranura específica, tiene las mismas bondades que los PCIE y maneja una velocidad de copia promedio desde 1,100 Mb/s sostenidos, existen los modelos SATA y NVMe

Ilustración 34 - Discos duros M.2

4.4 Hardware de informática forense

El hardware forense nos ayuda mucho a simplificar procesos y dar una certeza técnica adicional, que nuestro procedimiento se llevó a cabo con los más altos estándares, pero además con piezas tecnológicas destinadas para ello. Existen dos principales ramas de hardware que abordaremos, una de ellas son los dispositivos de hardware que pueden llevar a cabo la copia forense sin la necesidad de un equipo de cómputo ni de software adicional, así mismo existen dispositivos cuyo único fin es bloquear la escritura y garantizar que ni de forma adicional ni por accidente, se escriba en el medio original.

4.4.1 Bloqueadores de escritura

Para entender el funcionamiento, debemos verlos como un adaptador que crea un puente entre el disco origen y el equipo de cómputo que llevará a cabo el análisis o la copia forense.

Estos dispositivos nos darán una certeza a nivel físico, que el medio origen no será modificado, editado o alterado al momento de que se conecte a un equipo de cómputo, ya que esto es muy común que por accidente suceda, por

ejemplo, si conectase un disco duro de evidencia a mi equipo de cómputo, mi antivirus no analizará y podría modificar un fichero, con ello mi disco origen habría sido manipulado de forma incorrecta y si previamente se calculó el valor de integridad hash, este sería en un nuevo cálculo diferente, perdiendo con ello la certidumbre científica de no alteración, dos marcas de hardware reconocidas son:

- Wiebetech
- Tableau

Ilustración 35 – Bloqueadores Tableau

Ilustración 36 – Bloqueadores Wiebetech

4.4.2 Duplicadores

Cuando se busca tener alta portabilidad, los duplicadores forenses permiten que desde el propio dispositivo se lleve a cabo la copia forense, esto nos resulta muy beneficioso ya que no vamos a requerir un equipo de cómputo ni software instalado para llevar a cabo la tarea, solo basta conectar el disco origen, el disco destino por otro lado y tras un par de clics, seleccionando el formato de copia, el algoritmo hash empleado para validar el proceso, así como opciones avanzadas en cuanto a copias uno a uno, uno a dos, eliminación a bajo nivel de discos, entre otras opciones que cada fabricante incorpora, nuestro proceso de copia forense se llevaría a cabo.

Ilustración 37 – Duplicador Tx1 de Tableau

Ilustración 38 – Data Copy King II de SalvationData

4.5 Copia forense de discos duros

Cuando nos encontramos en nuestra laboratorio y vamos a proceder con la creación de una copia forense, tenemos que tener ya listo el disco que recibirá la copia, ya abordamos en capítulos previos la importancia de que este disco destino, esté formateado a bajo nivel para la certeza y tranquilidad de que nuestro procedimiento se llevó a cabo de la mejor manera.

Veremos que el procedimiento es muy similar entre todas las herramientas forenses, con pequeños cambios en la interfaz gráfica, todas las herramientas nos hacen la misma pregunta. ¿qué vamos a copiar, con que formato y hacia donde se debe guardar?

4.5.1 Copia forense con FTK Imager

1) El primer punto es seleccionar la opción de crear una imagen de disco

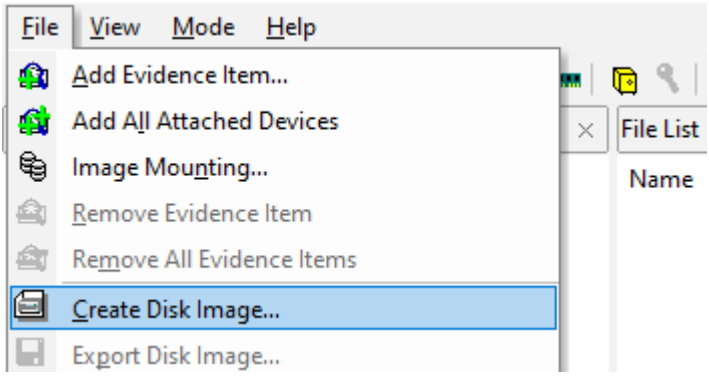


Ilustración 39 - Copia forense con FTK Imager

2) El siguiente paso sería seleccionar el tipo de evidencia que será nuestro objetivo

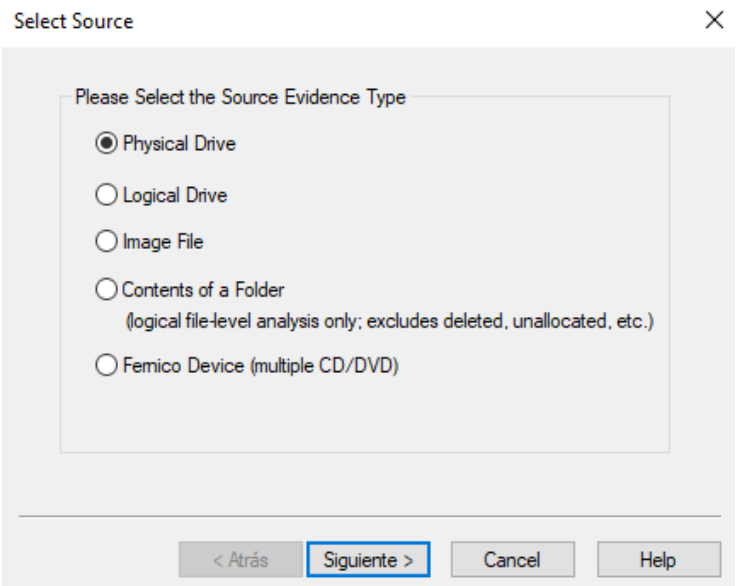


Ilustración 40 - Copia forense con FTK Imager

3) El sistema nos despliega las unidades que cumplen con el requisito previo y debemos seleccionar aquella que queremos copiar.

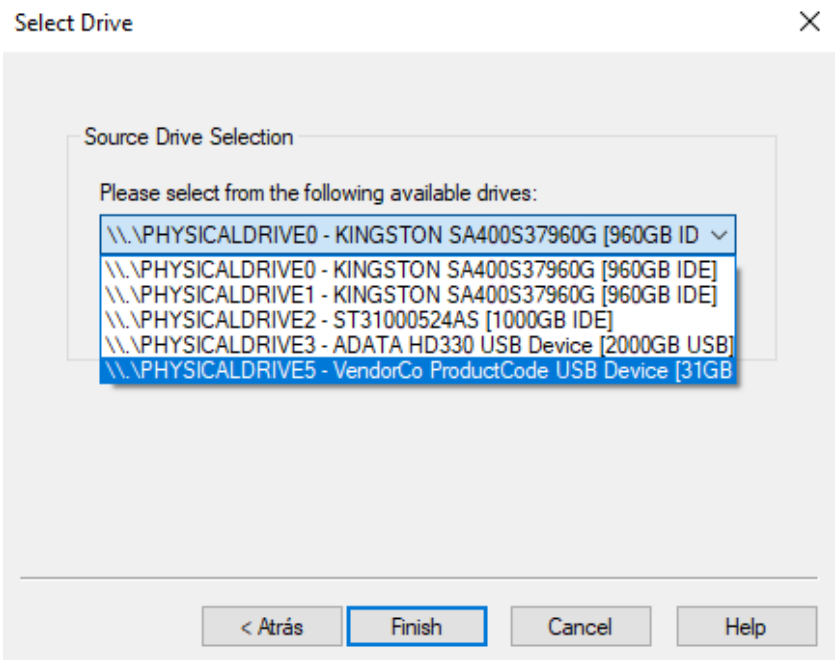


Ilustración 41 - Copia forense con FTK Imager

4) Posteriormente el sistema muestra un resumen de la tarea que llevará a cabo, tendremos que seleccionar “Add”, para indicarle en donde queremos arrojar la copia forense.

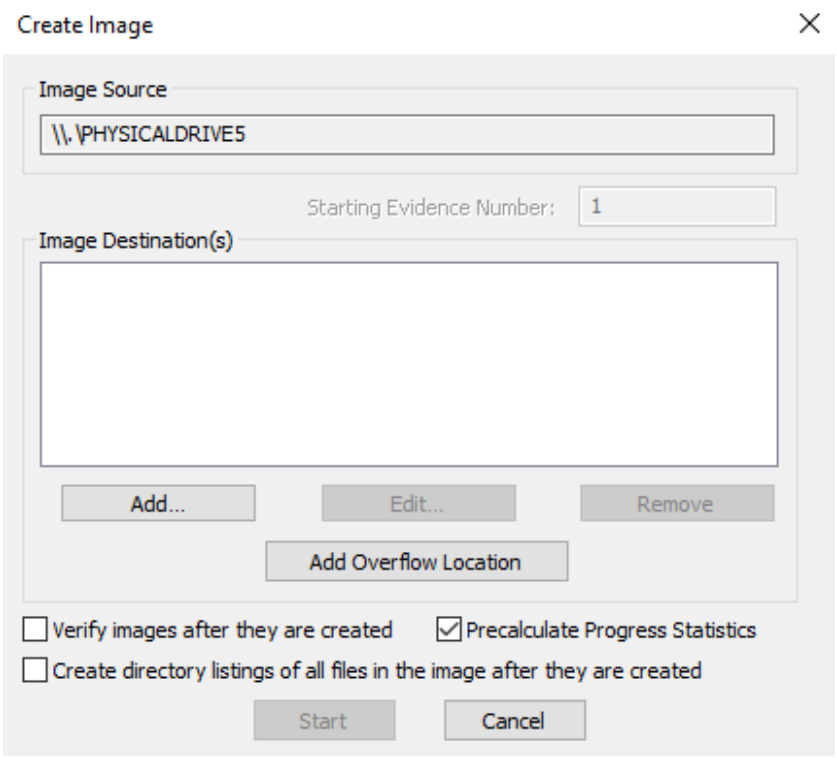


Ilustración 42 - Copia forense con FTK Imager

5) La aplicación nos preguntará el tipo de formato para nuestra copia forense.

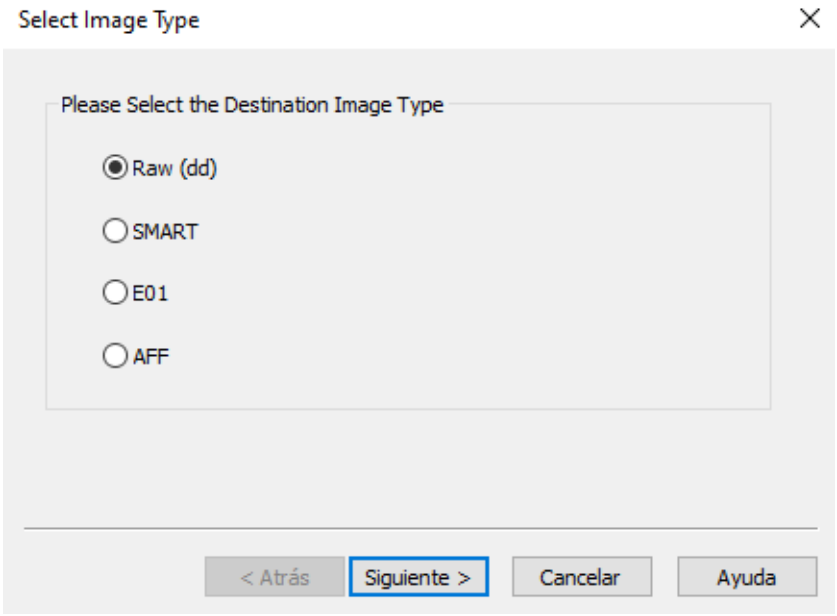


Ilustración 43 - Copia forense con FTK Imager

6) Casi para finalizar, tendremos que indicar exactamente en qué unidad y carpeta arrojaremos la copia, así como el nombre del archivo resultante. (opcionalmente podemos fragmentar la copia en pequeños ficheros de un tamaño que nosotros queramos)

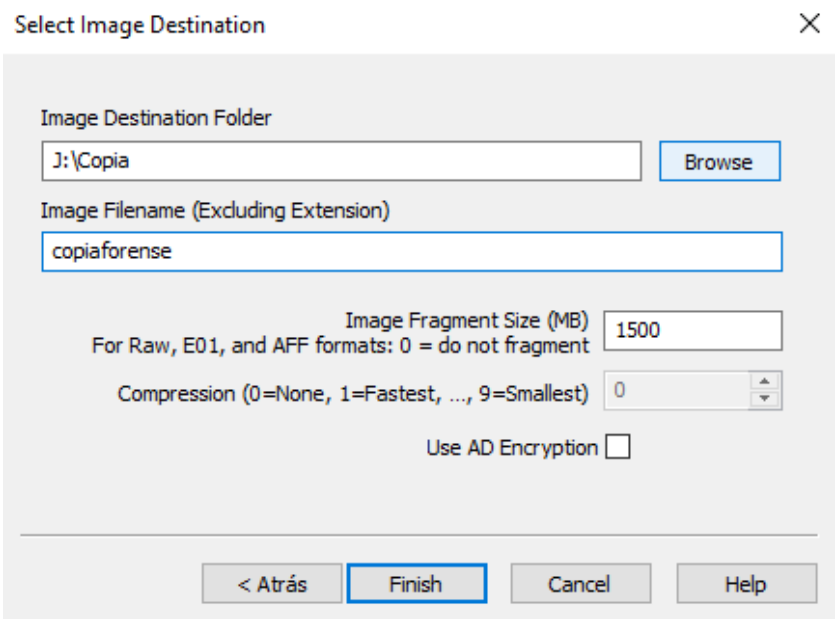


Ilustración 44 - Copia forense con FTK Imager

7) Como paso final, el sistema nos muestra el resumen completo, indicando el folder destino y opcionalmente podemos habilitar el precálculo del progreso, así como un listado de archivos encontrados y podríamos habilitar la verificación mediante hash, lo cual realiza un comparativo entre el origen y la copia resultante, para validar que la copia se realizó sin errores.

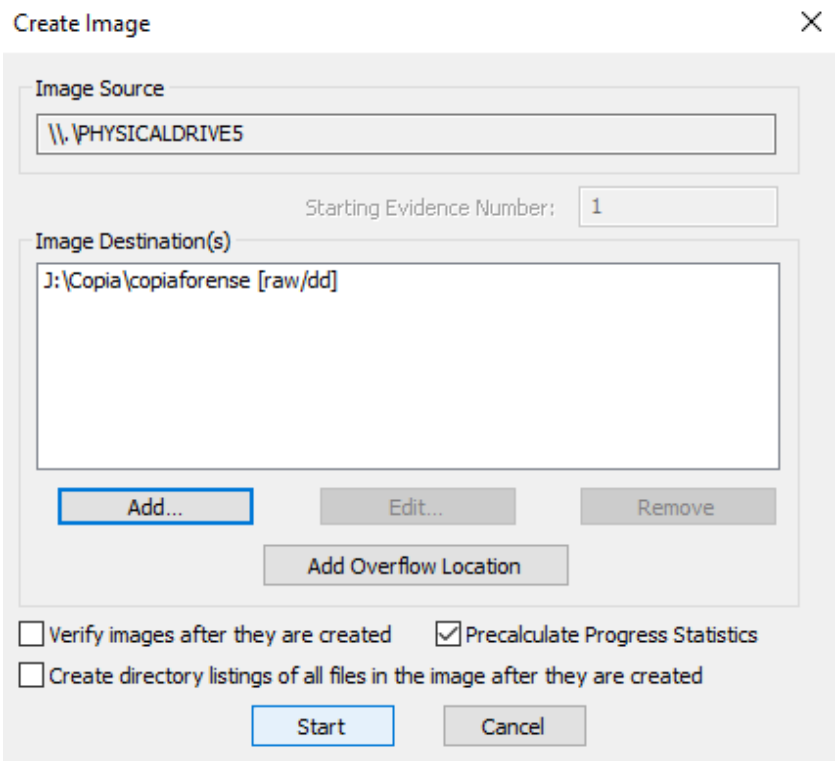


Ilustración 45 - Copia forense con FTK Imager

Cuando se hace una copia forense de un sistema encendido, no tiene ninguna utilidad que el proceso de validación sea habilitado, ya que el equipo encendido está trabajando, existen procesos, archivos abiertos, múltiples escrituras al disco duro y por consecuencia, siempre marcaría que la verificación no es correcta.

Mientras es llevado a cabo el proceso de copiado, podremos disponer de una barra de progreso, así como el tiempo faltante para finalizar.

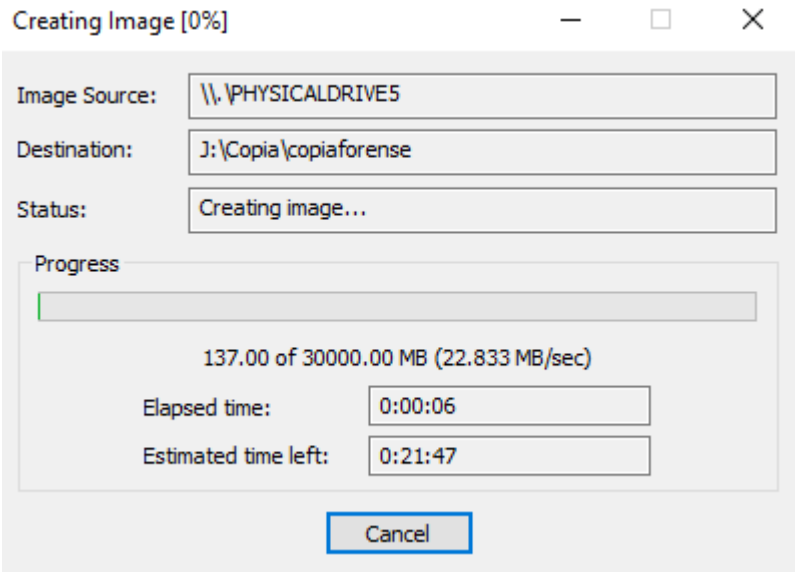


Ilustración 46 - Copia forense con FTK Imager

4.5.2 Copia forense con OSForensic

1) El primer punto es del menú principal, seleccionar “Create Forensic Image”

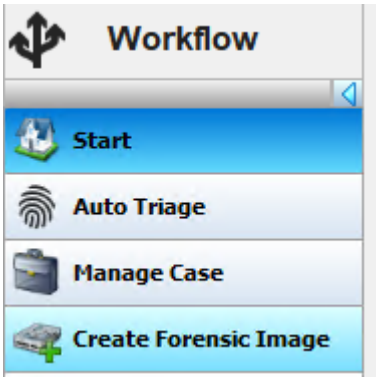


Ilustración 47 - Copia forense con OSForensic

2) Se nos abre una venta con opciones, en la cual la primera pestaña es la que requerimos, aquí tendremos que seleccionar en “Add” del menú inferior.

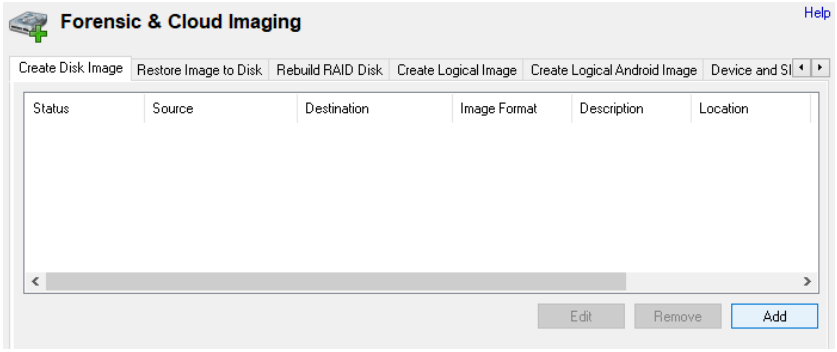


Ilustración 48 - Copia forense con OSForensic

3) Una nueva ventana nos permitirá seleccionar como primer punto el disco origen, podremos elegir entre discos completos o particiones, la ruta destino para alojar la copia forense, de igual forma podemos habilitar o deshabilitar la opción de verificar la imagen, así como el algoritmo que queremos emplear para validar la copia forense.

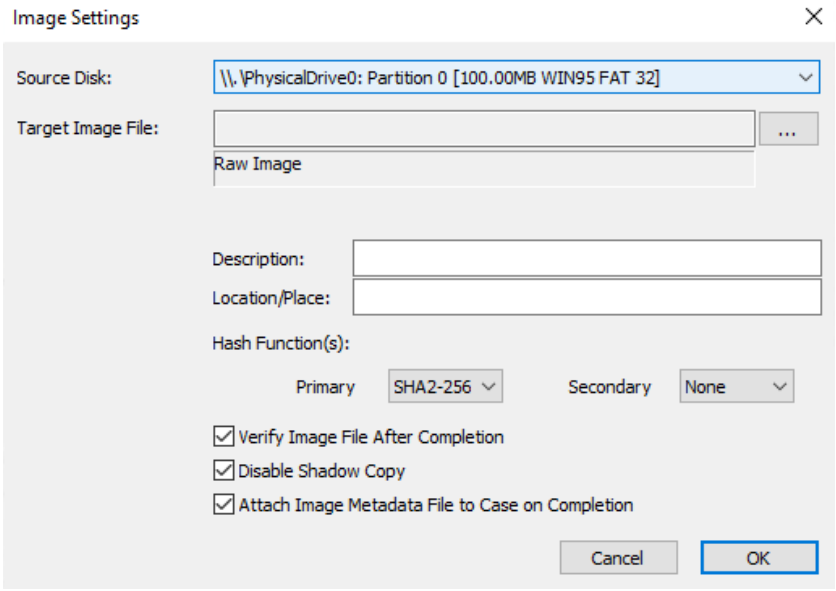


Ilustración 49 - Copia forense con OSForensic

4.5.3 Copia forense con HelixPro

La herramienta “Helix 3 Pro” pese a que se lanzó en 2009, cumple al día de hoy su objetivo, con una serie de aplicaciones portables incluidas nos va a permitir extraer la memoria RAM, pero también obtener un reporte con el estado general del sistema que en nuestra laboratorio podremos analizar y tomar de ahí un punto de partida al comenzar en el análisis profundo.

1) Debemos seleccionar del menú izquierdo, un disco duro que será el que copiaremos.

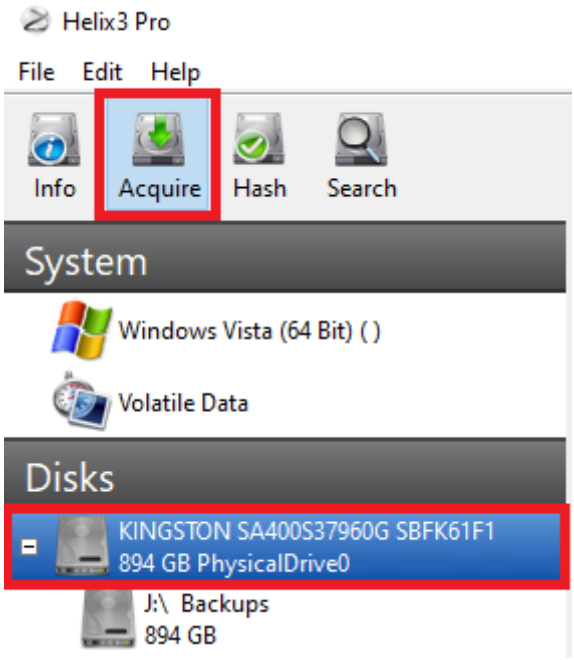


Ilustración 50 - Copia forense con HelixPro

2) Con ello el menú superior habilita la opción adquirir evidencia.
3) Una vez hecho esto, el programa nos mostrará las opciones de configuración de la copia forense, entre ellas podremos elegir el formato de copia, el tamaño de segmentación (si así lo queremos), el algoritmo usado para validar la copia y por último el destino de la misma, la cual como recordaremos, debe ser un medio de almacenamiento que esté limpio y libre de

registros o datos antiguos (previo formateo a bajo nivel o formateo lento).

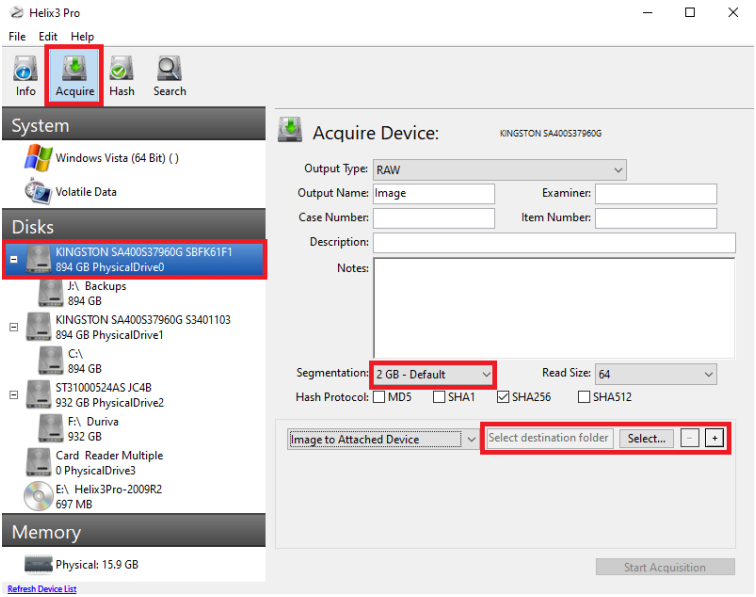


Ilustración 51 - Copia forense con HelixPro

4.6 Copia forense desde Linux

1) Como primer paso debemos identificar los discos existentes, particiones y punto de montaje, para ello con el comando “lsblk” podemos obtener la información del sistema

```
forense@Tequila:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0  200G  0 disk
├─sda1   8:1    0  198G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0    2G  0 part [SWAP]
sdb      8:16   0  102M  0 disk /media/disco-nuevo
sr0     11:0    1 1024M  0 rom
```

Ilustración 52 – Listado de unidades y puntos de montaje en Linux

2) Con el comando “dd”, podemos llevar a cabo la copia forense, solo es necesario indicar que queremos copiar y donde lo queremos arrojar.

Ilustración 53 – Copia forense en Linux con dd

3) De forma opcional, pero altamente recomendado es agregar al comando “conv=noerror,sync bs=512”, con ello conseguimos indicarle a la aplicación, que en caso de error de lectura del disco por sectores dañados o inaccesibles no sea detenido el proceso, así como el tamaño de bloque que evita en lo posible transferir segmentos dañados.

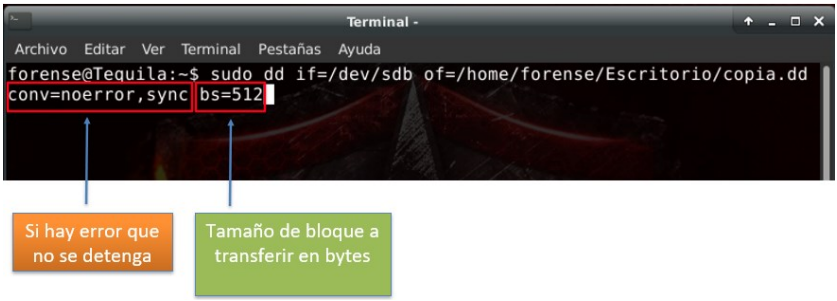


Ilustración 54 – Copia forense en Linux con dd

4.7 Copia forense en vivo, sistemas Windows

Como ya hemos abordado anteriormente, es posible que el equipo de cómputo que tengamos enfrente y encendido esté cifrado, por ello si apagamos el sistema, nos enfrentaremos al problema de tener una unidad cifrada y cuya contraseña es indispensable para poder llevar a cabo nuestra investigación.

En la medida de lo posible, se recomienda tener el equipo de cómputo apagado, desconectar los discos y llevar uno a uno la copia forense, sin embargo, hay situaciones que al llegar a sitio encontramos un equipo de cómputo encendido y tras un breve análisis detectamos que no es viable llevar a cabo la copia forense apagando y desconectados uno a uno de los discos, por ejemplo:

- El equipo de cómputo es crítico y no es posible apagarlo.

- El sistema está montado en un arreglo RAID y se desconoce la arquitectura de este.
- El equipo está cifrado, es indistinto si es BitLocker, TrueCrypt, FileVault o cualquier sistema de cifrado de disco (se realiza la copia de la partición).

De los pasos descritos en la copia forense de discos, el cambio que tendríamos sería en el punto 3, ya que tendríamos que seleccionar nuestro disco duro principal, por lo regular es el descrito como PHYSICALDRIVE0, sin embargo, debemos verificar ya sea por tamaño o desde la utilidad de discos, el orden de los mismos para estar seguros de que se está copiando el disco asociado con el sistema Windows que tenemos encendido.

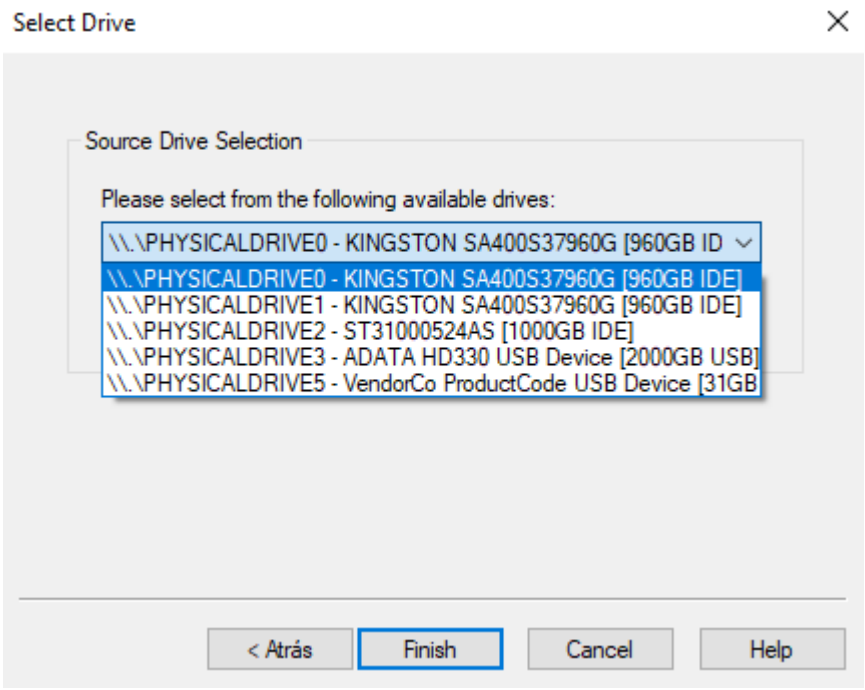


Ilustración 55 - Copia forense en vivo, sistemas Windows

4.7.1 Detección de unidades cifradas

Es importante revisar antes de apagar si el equipo de cómputo que tenemos a la vista está o no cifrado, si fuera el caso que lo esté, debemos corroborar con el dueño del equipo o la gente de sistemas si conocen la contraseña para descifrar el disco, esto es algo que debemos corroborar antes del apagado y sugiero pedir la firma de un

documento que señale que el cliente conoce la contraseña, con el fin de evitar cualquier futuro problema o mal entendido.

Si se detecta que el disco sí está cifrado y no se tiene la contraseña, tendríamos que en ese mismo momento llevar a cabo la copia forense de la unidad, así conseguimos tener una copia del disco con todos los datos disponibles, una vez que el equipo es apagado, ya no podremos acceder a estos registros y nuestra copia forense sería la única fuente accesible de información del caso.

Una de las herramientas que prefiero para la detección de unidades cifradas es MAGNET Encrypted Disk Detector[5] ya que con un solo clic realiza una revisión de los discos duros y nos indica si uno de ellos se encuentra con algún tipo de cifrado

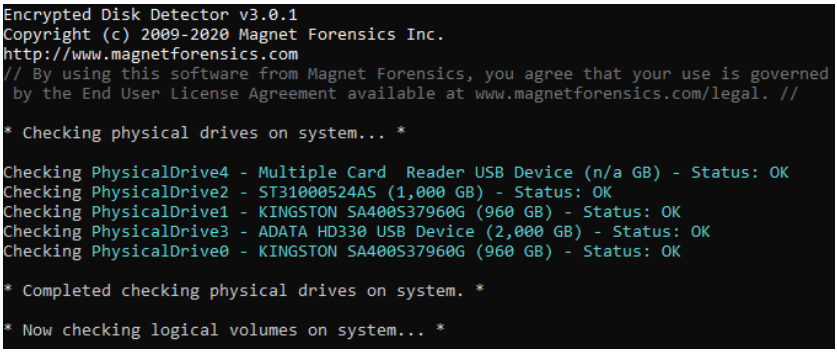


Ilustración 56 - Detección de unidades cifradas con MAGNET

[5] https://www.magnetforensics.com/resources/encrypted-disk-detector/

En este punto me interesa que no solamente dependamos de una herramienta, sino que conozcamos y tengamos la certeza de por qué una herramienta nos está indicando un resultado y no solo aprender a dar clic, por ello veremos mediante el uso de la herramienta FTK Imager[6], el procedimiento manual para analizar las unidades, podemos agregar como evidencia el disco duro del que sea desea conocer si se encuentra cifrado.

El procedimiento es el siguiente, desde el panel de opción de selecciona “Add Evidence item…”

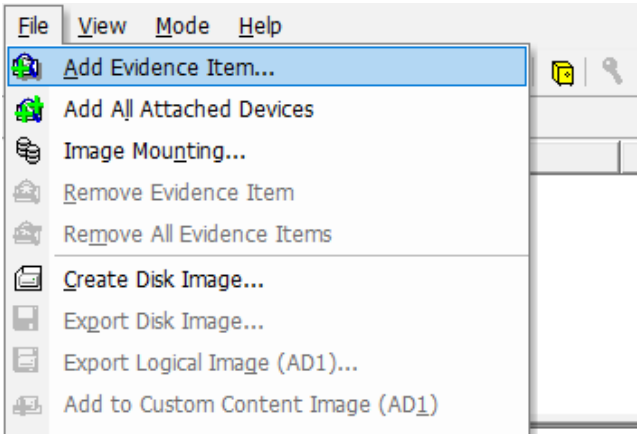


Ilustración 57 - Detección de unidades cifradas con FTK

[6] https://accessdata.com/product-download/

Con lo cual el sistema nos genera la siguiente ventana, sobre la cual debemos seleccionar “Physical Drive”.

Ilustración de detección de unidades cifradas con FTK Imager

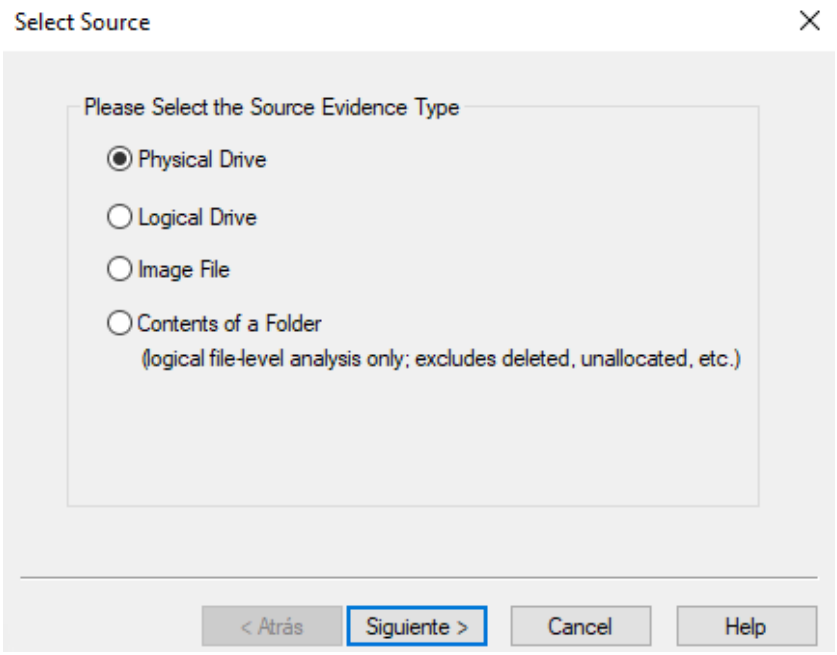


Ilustración 58 - Detección de unidades cifradas con FTK

Para posteriormente indicar cual, de los dispositivos de almacenamiento conectados, será el que queremos analizar.

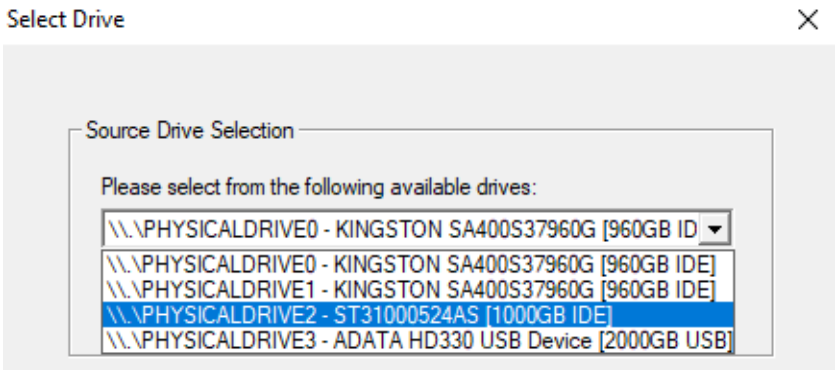


Ilustración 59 - Detección de unidades cifradas con FTK

Al finalizar el proceso de agregar la unidad, el punto clave es al desplegar la información del disco, ya que FTK Imger lee las unidades y nos indica el sistema de archivos que contiene cada partición, en circunstancias “normales” y me refiero al resultado de realizar una instalación manual con los valores por default de Windows, se debe visualizar algo similar a esto.

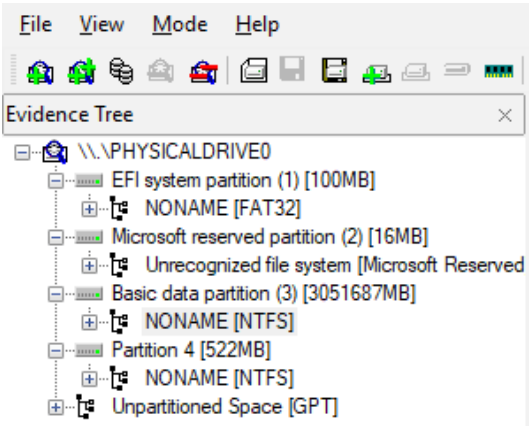


Ilustración 60 - Detección de unidades cifradas con FTK

Podemos ver que se listan las particiones con un número (1) seguidas del tamaño que le corresponde. Las primeras son muy pequeñas, de 100 y 16 Mb relativas el sistema operativo Windows que las crea al momento de llevar a cabo la instalación, sin embargo, la que nos es de relevancia en este caso, es la de mayor tamaño de 915075 Mb y con nombre “Basic data partition”, en esta partición podemos ver que en la fila debajo, se indica “NONAME” [NTFS], el valor de NTFS nos dice que la herramienta FTK pudo identificar el sistema de archivos y podría listar todos los elementos que contiene la unidad.

Al desplegar el árbol de evidencia, veremos un listado de archivos lo cual nos permite concluir que la unidad NO está cifrada

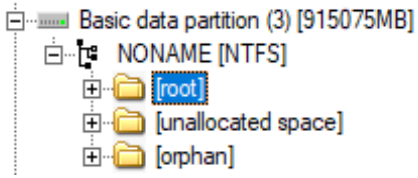


Ilustración 61 - Detección de unidades cifradas con FTK

Si la unidad sí estuviera cifrada, en el campo de la partición con mayor tamaño, se mostraría el texto “unrecognized file system [Data]”. Siendo imposible para la aplicación desplegar el árbol de archivos contenidos, ahí, de inmediato podíamos concluir que la unidad sí está cifrada y requerimos llevar a cabo la copia forense en lo que se

conoce como “en vivo”, que es el proceso de copiar el disco duro sin apagar el sistema operativo. *El proceso de copia forense se describe en un tema posterior.*

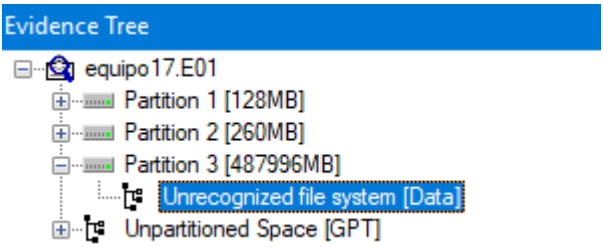


Ilustración 62 - Detección de unidades cifradas con FTK

De no llevar la copia en eso momento la copia del “logical drive”, es cuando en nuestro laboratorio queramos analizar los elementos del disco, montando la unidad o agregándola como evidencia, veremos a la unidad con un candado como se muestra en la imagen.

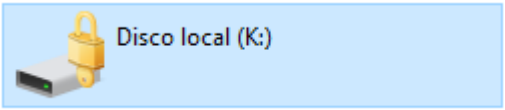


Ilustración 63 - BitLocker

El problema al que nos enfrentaríamos de no haber llevado la copia de la unidad sería llevar a cabo un ataque de fuerza bruta para conseguir los 48 dígitos de la contraseña.

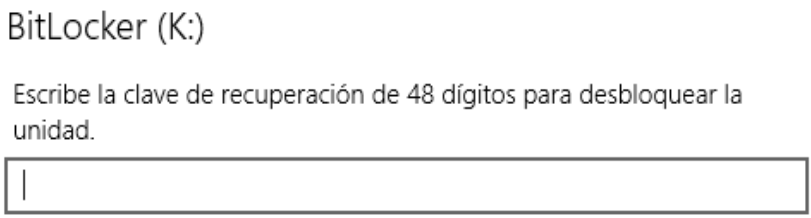


Ilustración 64 - BitLocker

Si se detecta que el disco NO está cifrado, podemos proceder con el apagado del equipo de cómputo.

4.7.2 Copia forense en vivo, entornos Windows cifrados

Como ya hemos abordado anteriormente, es posible que el equipo de cómputo que tengamos enfrente y encendido esté cifrado, por ello si apagamos el sistema, nos enfrentaremos al problema de tener una unidad cifrada y cuya contraseña es indispensable para poder llevar a cabo nuestra investigación.

Si fuera el caso que el sistema esté cifrado, el procedimiento es muy similar al explicado en los descritos en la copia forense de discos, sin embargo, solo existe un cambio en el punto 2, al momento de seleccionar el tipo de copia forense, ya que, en lugar de seleccionar como objetivo el dispositivo físico, debemos seleccionar “Logical Drive”

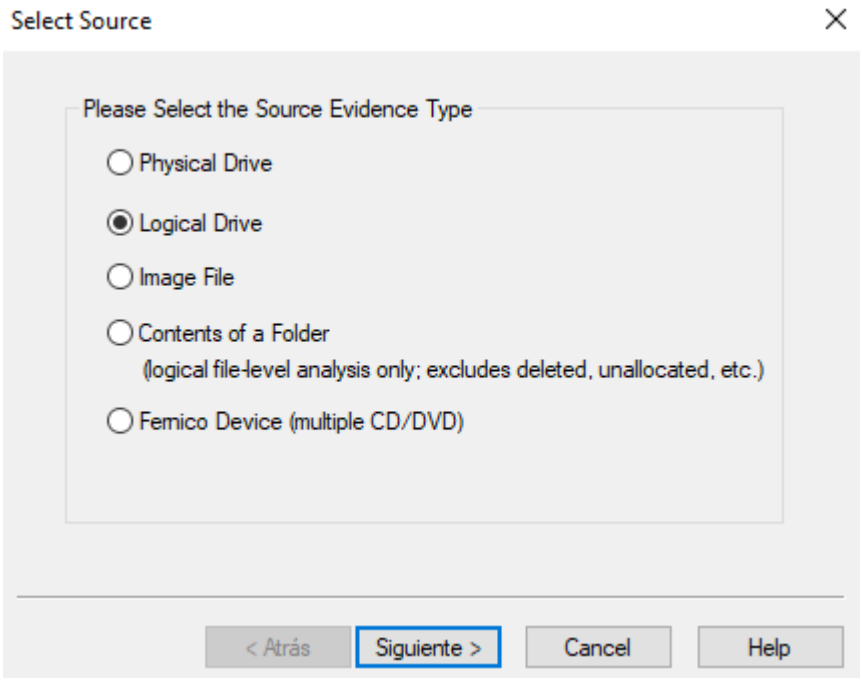


Ilustración 65 - Copia forense en vivo, entornos Windows cifrados

Este pequeño cambio en el procedimiento nos muestra las letras de las unidades que están disponibles, es aquí donde seleccionamos la unidad C:

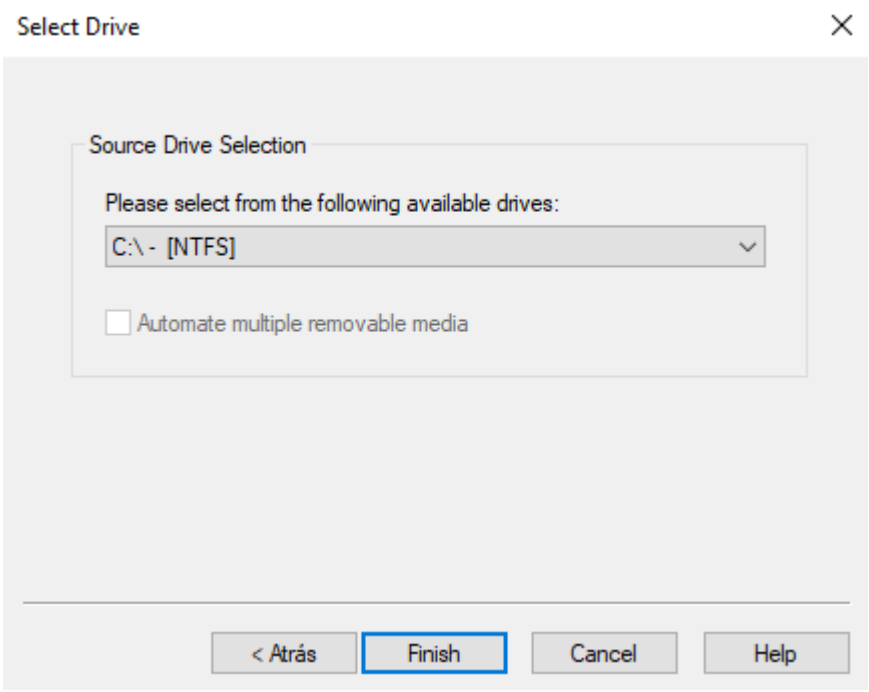


Ilustración 66 - Copia forense en vivo, entornos Windows cifrados

Los demás pasos son exactamente iguales los descritos en el tema de la copia forense de discos, sin embargo, el resultado será una copia de la unidad sin cifrar y disponible para que podamos acceder a todos los datos almacenados.

Es importante entender que físicamente una unidad que fue cifrada siempre lo estará (salvo que se le desactive el cifrado), sin embargo, a nivel tecnológico, cuando se coloca la contraseña para visualizar o arrancar la unidad, de forma virtual la aplicación BitLocker, TrueCrypt, FileVault o cualquier que fue empleada, crea de forma virtual un disco

con los datos accesibles, en nuestro caso la unidad C: existe solo de forma virtual, por ello, es imprescindible que si está encendido el equipo y ya detectamos el cifrado, hagamos cuanto antes este tipo de copias forenses.

4.8 Cálculo de hash en Windows

Como vimos en los primeros temas, el valor de integridad hash es el tema central en la preservación de evidencia, por ello podremos encontrar múltiples programas que nos permiten obtener este cálculo de forma muy rápida.

4.8.1 CMD

El propio sistema operativo Windows de forma nativa puede llevar a cabo el cálculo de algoritmos hash, la herramienta certutil pese a que su objetivo es manejar certificados digitales y diversos procesos, podemos emplearla para calcular un valor hash, para ello la sintaxis es muy simple:

certutil -hashfile <ruta del archivo> SHA256

Resultado

```
F:\>certutil -hashfile exiftool.exe SHA256
SHA256 hash de exiftool.exe:
4dcf9f42853154f481a43ebdb909631da5eb0ed20292693282906d54c51a3e68
CertUtil: -hashfile comando completado correctamente.
```

Ilustración 67 – Cálculo del valor hash desde CMD con Certutil

4.8.2 PowerShell

Con una sencilles similar a CMD, desde PowerShell podremos realizar el cálculo de valores hash, para ello usaremos el comando “Get-FileHash”, la sintaxis sería:

Get-FileHash <ruta del archivo> -algorithm <algoritmo>

```
PS F:\> Get-FileHash exiftool.exe -algorithm sha256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          4DCF9F42853154F481A43EBDB909631DA5EB0ED20292693282906D54C51A3E68       F:\exiftool.exe
```

Ilustración 68 – Cálculo del valor hash desde PoweShell

4.8.3 Multihasher

Esta herramienta es gratuita y portable (existe la versión de instalación), la cual tiene un solo objetivo y lo cumple a perfección, calcular el valor hash que indiques de un archivo o de todo un directorio, para ello es necesario seleccionar el algoritmo que se desea emplear; MD5, SHA1, SHA256, SHA384, SHA512 y darle al programa el archivo o directorio del cual queremos realice el proceso de cálculo, con ello nos irá mostrando una barra de

progreso que al llegar al 100% no arroja cada uno de los valores hash resultantes.

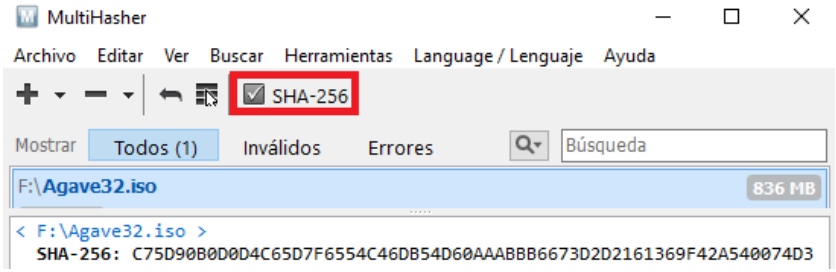


Ilustración 69 – Cálculo hash con Multihasher

4.8.4 OSForensic

La herramienta tiene un módulo llamado “Create Hash”, es aquí donde debemos seleccionarlo para pasar a la ventana de cálculo

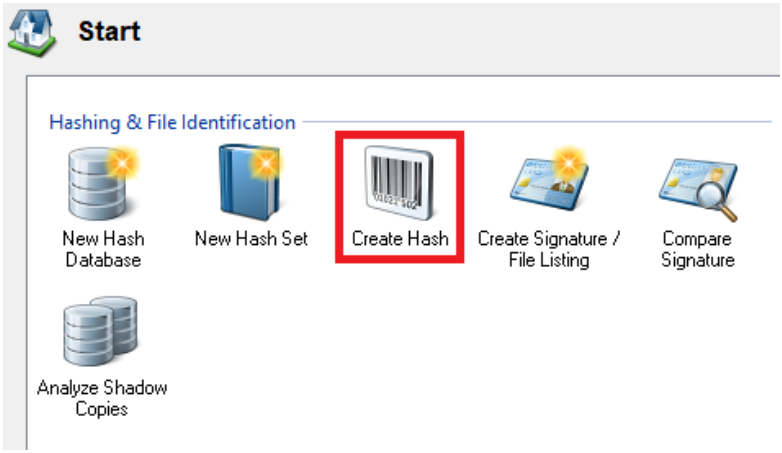


Ilustración 70 – Cálculo hash con OSForensic

La herramienta tiene opciones adicionales a multihasher, como lo es poder elegir entre calcular el valor a un archivo, a un volumen o bien, a un texto, además de poder decidir el algoritmo que deseamos emplear para el cálculo y optativamente un segundo algoritmo si así lo quisiéramos

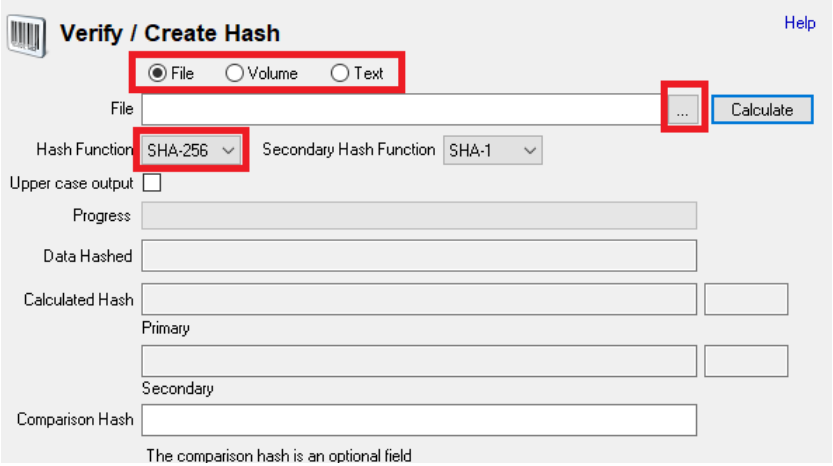


Ilustración 71 – Cálculo hash con OSForensic

4.9 Cálculo de hash en Linux

Todas las distribuciones Linux nos permiten de forma nativa calcular el valor hash de un fichero o directorio de una forma bastante sencilla y similar a lo que vimos con CMD y PowerShell

La sintaxis es:

<algiritmo>sum /ruta

En algoritmo puede ser md5, sha1, sha256, sha512 por ejemplo:

sha256sum /home/archivo.txt

sha1sum /home/archivo.txt

md5sum /home/archivo.txt

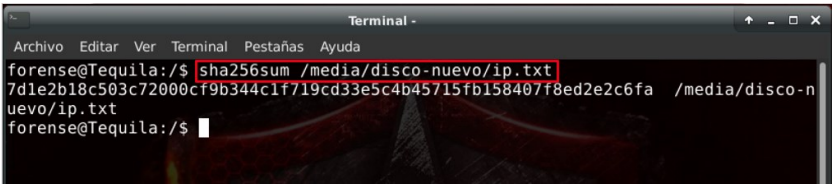


Ilustración 72 - Cálculo hash desde Linux

El resultado del cálculo como se observa se muestra en pantalla, por lo que el procedimiento es muy simple.

5. Laboratorio forense

Es muy importante que nuestro laboratorio forense esté configurado para una alta demanda, pero muy importante, evitando esos cuellos de botella que, al iniciar en la informática forense, por desconocimiento llegamos a generar embudos que aumentan el tiempo de procesamiento.

Contar con tres discos duros sería un escenario ideal para comenzar, en el siguiente gráfico vemos la configuración recomendada.

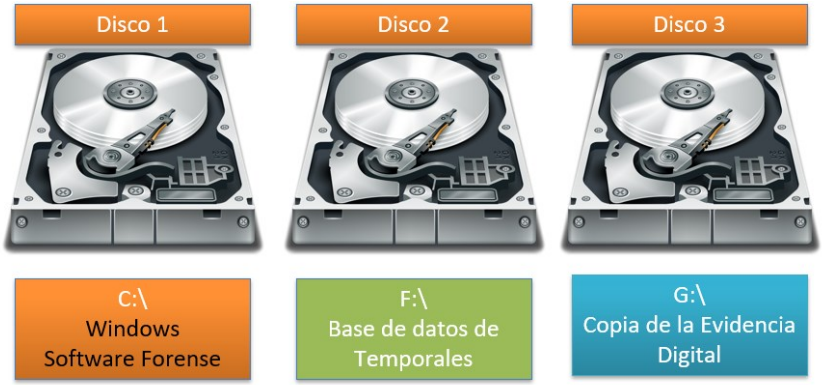


Ilustración 73 - Laboratorio forense

Disco 1: En este disco duro tendremos nuestro sistema operativo (Windows o Linux) y los programas informáticos

que utilizaremos, es altamente recomendado que sea un SSD.

Disco 2: Cada vez que hacemos uso una suite forense como Autopsy, OSForensic, EnCase, FTK, Nuix, entre otras, las herramientas crean una base de datos en la cual volcarán todos los datos que se generen del proceso de investigación, este disco duro se destina para ello, es el disco que tendrá la mayor taza de transferencia y uso. (Las herramientas comerciales permiten destinar un disco duro adicional para descomprimir los archivos que lo requieran, así como para desempaquetar los ficheros PST y OST)

Disco 3: Nuestra evidencia digital estará almacenada en este disco duro, ya sea una copia forense completa, parcial o de objetivos, este disco duro solo tendrá almacenada la evidencia digital, la velocidad de lectura de este disco no será muy alta, ya que las herramientas procesan la información poco a poco, por ello un disco SSD no sería indispensable, pero si ayuda a mejorar ligeramente el rendimiento.

Bajo este modelo de trabajo podemos tener la tranquilidad de que no se harán cuellos de botella a nivel discos duros, en lo que respecta al procesador y la cantidad de memoria RAM la recomendación es siempre contar cuando menos con 2 Gb por cada uno de los núcleos del procesador, de ser posible contar con procesadores Xeon por la cantidad

de núcleos y subprocesos que entrega, así como la cantidad de memoria RAM que soporta.

5.1 Suite forense gratuita

Como primer punto debemos aclarar la diferencia entre Suite Forense y una distribución forense, la primera, es un programa que contiene las herramientas necesarias para automatizar el proceso de investigación, por otro lado, una distribución forense, es una versión de un sistema operativo orientada precisamente a la informática forense y a su vez, puede contener una Suite Forense.

La suite forense por excelencia dentro de los programas gratuitos es Autopsy Forensic, este programa consiguió reunir bajo una interfaz gráfica los programas de “The Sleuth Kit”, además de los que la misma comunidad ha desarrollado y liberado a lo largo del tiempo, estos programas con funcionalidades adicionales se conocen como módulos y nos permiten realizar una serie de tareas específicas dentro de nuestro proceso de investigación.

Las distribuciones forenses más representativas son: Caine, DEFT, SIFT, Tequila SO (desarrollada por el autor de este libro, por lo que no podía faltar en este listado) y Tsurugi, cada una de ellas incorpora lo que sus respectivos desarrolladores consideran las mejores herramientas para el proceso de investigación como laboratorio forense, no

puede faltar Autopsy dentro de estas distribuciones, y una serie de aplicaciones libres para llevar a cabo copias forenses, análisis de metadatos, interpretación de archivos de sistema, visores hexadecimales, clasificación de archivos por tiempos MAC, interpretación de ficheros $MFT entre otras tantas aplicaciones que iremos viendo de forma gradual.

5.2 Autopsy Forensic

Como lo mencionamos previamente, esta es la suite forense más importante por lo potente que resulta ser el proceso automatizado que tienen sus módulos y madurez del desarrollo.

En las primeras versiones la interfaz gráfica resultaba ser mediante un puerto en concreto dentro del navegador con una forma de trabajo como esta:

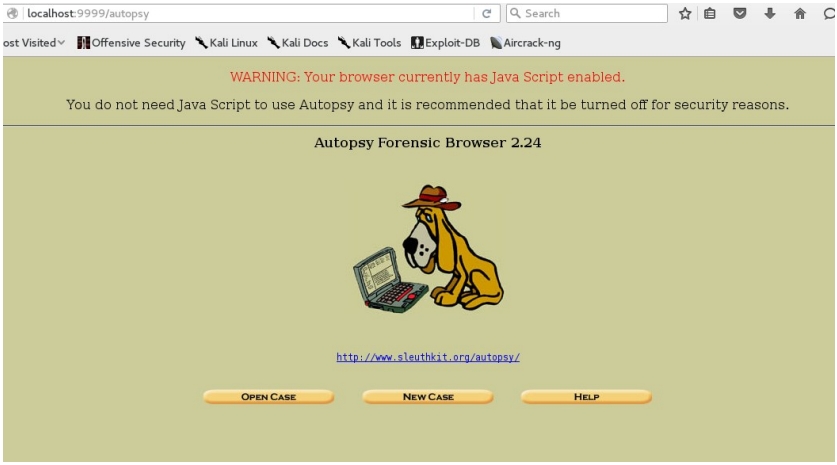


Ilustración 74 - Autopsy Forensic

Hoy en día resulta una herramienta muy sólida que corre en Java, por lo que es multiplataforma, pero sobre todo tiene una interfaz gráfica bastante intuitiva que iremos viendo.

5.2.1 Crear un caso

Iniciando la herramienta Autopsy Forensic se nos muestra una ventana con 3 opciones, sobre la cual tenemos que elegir “Create New Case”

Ilustración 75 - Autopsy Forensic

Inmediatamente nos abrirá una ventana para ir llenando los datos del nuevo caso, aquí es fundamental señalar que la ruta del “Base Directory” se debe encontrar en un medio de almacenamiento independiente de todo; independiente del sistema operativo, independiente del disco duro que contenga la copia forense, un disco duro únicamente reservado para almacenar archivos temporales. (esto ya fue abordado al inicio del tema 5)

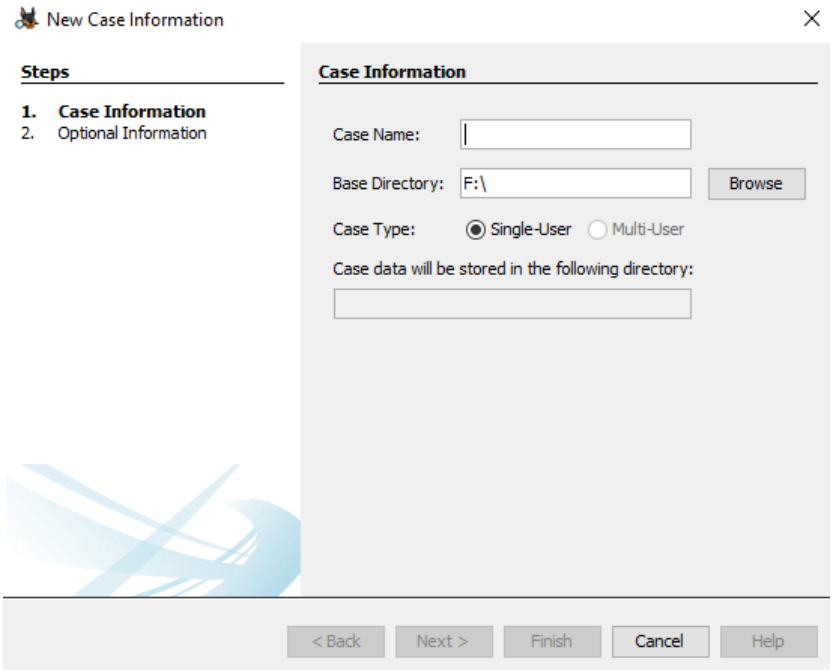


Ilustración 76 – Crear un caso en Autopsy Forensic

Una vez llenados los datos procedemos con el botón siguiente.

De forma opcional podemos llenar los datos generales del caso, que si llevamos muchas investigaciones simultaneas no s será de gran ayuda.

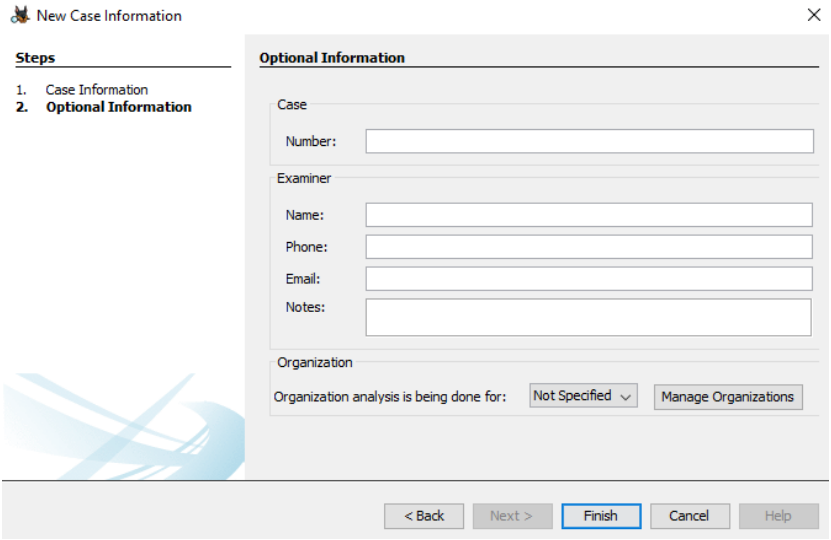


Ilustración 77 – Crear un caso en Autopsy Forensic

5.2.2 Agregar el tipo de evidencia

- Autopsy Forensic, nos permite elegir entre distintos tipos de evidencia como:
- Discos de imagen (copias forenses) y máquinas virtuales
- Discos físicos conectados
- Particiones de discos
- Solo analizar el espacio no alojado de una copia forense
- Reportes pre generados de Autopsy/XRY

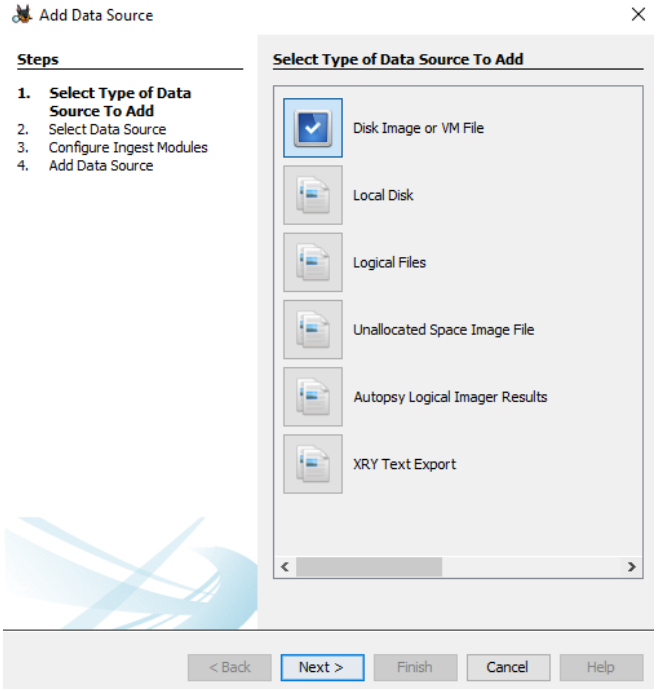


Ilustración 78 – Crear un caso en Autopsy Forensic

El siguiente punto es indicar la ruta de la evidencia.

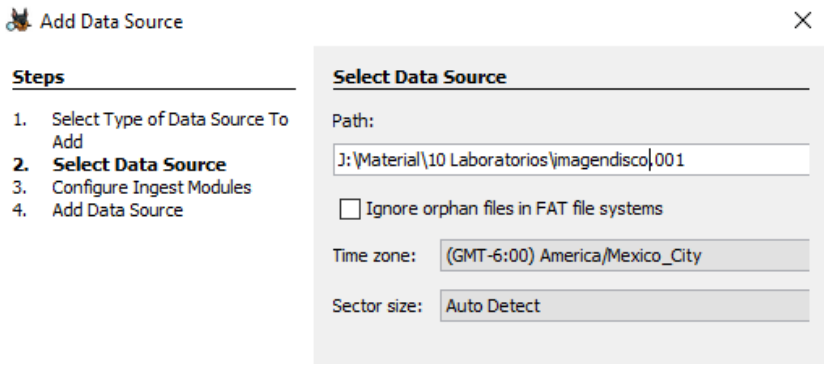


Ilustración 79 – Crear un caso en Autopsy Forensic

5.2.3 Módulos

El siguiente paso es el más importante, ya que elegiremos los módulos que deseamos aplicar sobre la evidencia, de forma nativa se encuentran todos los módulos seleccionados, sin embargo NO LO RECOMIENDO, lo ideal es solo habilitar los módulos que requiramos de forma inicial, en muchas ocasiones es posible llegar a un resultado sin procesar toda la evidencia, por ejemplo, podríamos analizar sólo la actividad del usuario y esto nos podría dar información que nos permite resolver el caso, con ello ahorramos muchas horas de trabajo.

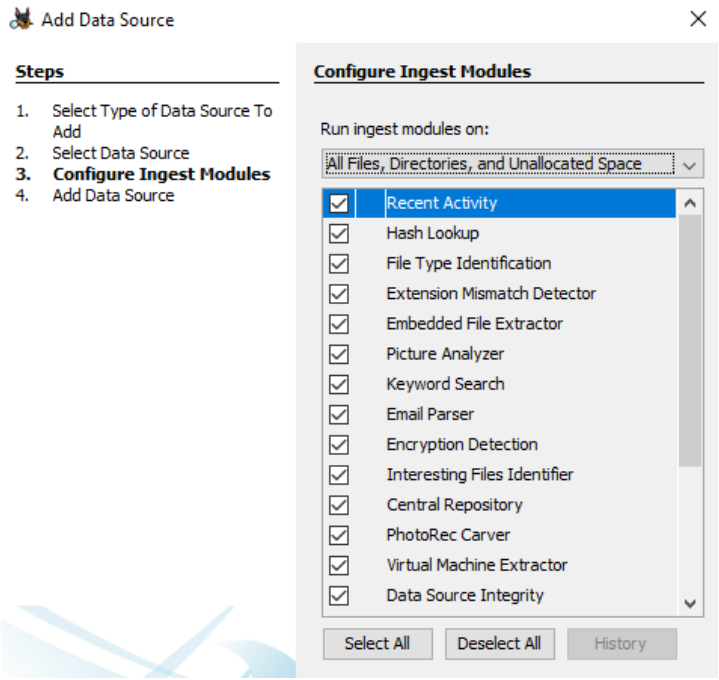


Ilustración 80 – Módulos en Autopsy Forensic

Esto no debe ser interpretado que solo ese módulo es funcional, sino que podemos ejecutar un módulo, ver el resultado y si la información obtenida no es suficiente, podremos ejecutar módulos subsecuentes, **sin tener que habilitar todo y tener que esperar días hasta que se termine de procesar la evidencia.**

En este libro no abordaremos cada uno de los módulos, ya que la página oficial de Autopsy tiene la descripción detallada de cada uno de ellos.

IMPORTANTE: El antivirus de nuestro equipo de cómputo, debe considerar el directorio de la copia forense y el directorio de temporales en sus exclusiones, ya que, de no ser así, podría el antivirus eliminar archivos que están siendo analizados y el resultado de Autopsy Forensic sería incompleto.

Tras unos instantes se mostrará el proceso de la evidencia que fue agrada, esto proceso puede demorar un par de minutos, sin embargo, cuando termina, solo terminó de agregar la evidencia, el procesamiento apenas está comenzando.

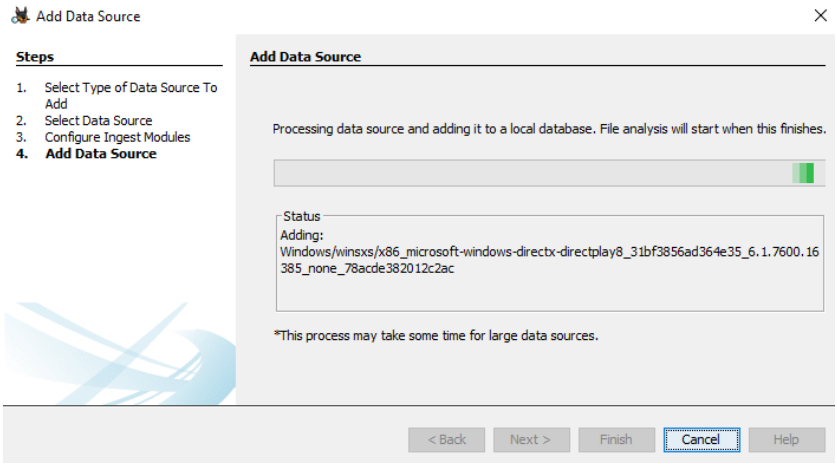


Ilustración 81 – Procesamiento en Autopsy Forensic

En la parte inferior izquierda podremos ir viendo el progreso general de cada uno de los módulos que seleccionamos,

aquí dependiendo de las características de hardware con las que contemos, el tamaño de la copia forense, así como el número de módulos podrá ser un par de horas hasta un par de días o semanas, es importante no causar cuellos de botella por lo que hago énfasis en usar cuando menos 3 discos duros en este proceso, como detallé al inicio del módulo 5.

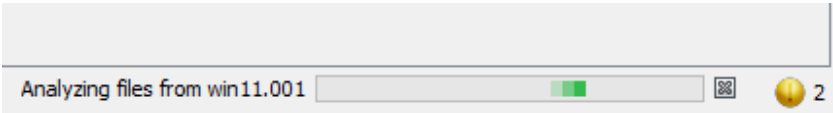


Ilustración 82 - Procesamiento en Autopsy Forensic

5.2.4 Visualización de evidencia

Conforme el progreso de los módulos vaya avanzando, podremos ver que, en la parte lateral izquierda, los resultados de la evidencia se irán llenando y aparecen nuevas categorías, las cuales poco a poco se irán llenando.

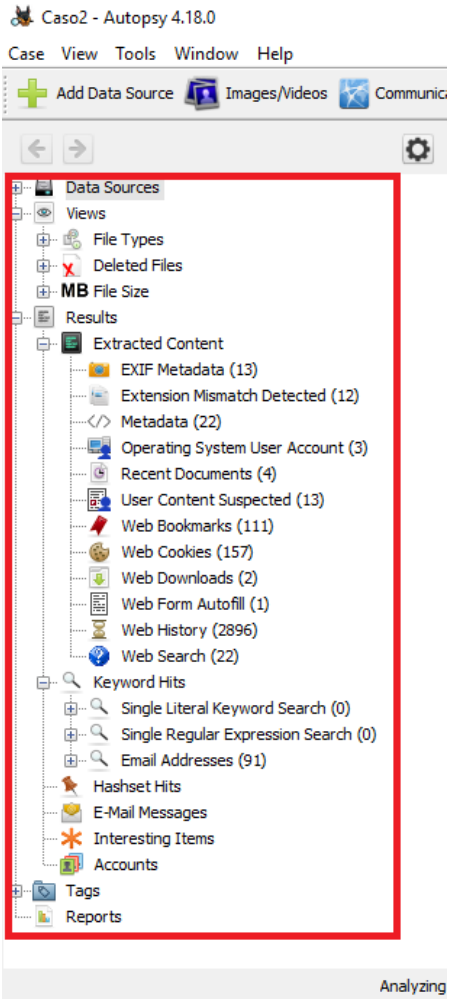


Ilustración 83 - Visualización de evidencia en Autopsy

Recomiendo encarecidamente que al navegar en estas secciones mientras el progreso del análisis avanza, la navegación sea lo más lenta y de ser posible restringirla

hasta la finalización de los módulos, ya que nuestro procesador muy probablemente debe estar trabajando a máxima potencia y navegar en las diversas categorías, lo cual podría conducir a que el programa deje de responder y falle el progreso completo, por ello solo consultar datos puntuales o esperarnos a que haya terminado.

Al finalizar el procesamiento de los módulos, podremos ver que Autopsy Forensic pudo clasificar la evidencia con categorías como tipos de archivos, eliminados y por tamaños

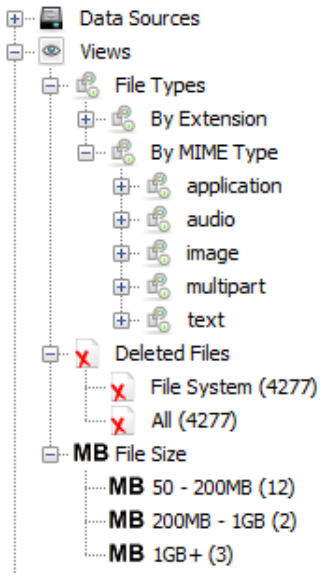


Ilustración 84 - Visualización de evidencia en Autopsy

Además, por supuesto, de cada una de las categorías de clasificación que nos van a permitir pasar de cientos de miles o millones de archivos que contiene la copia forense en datos segmentados, sobre los cuales podremos ir analizando poco a poco.

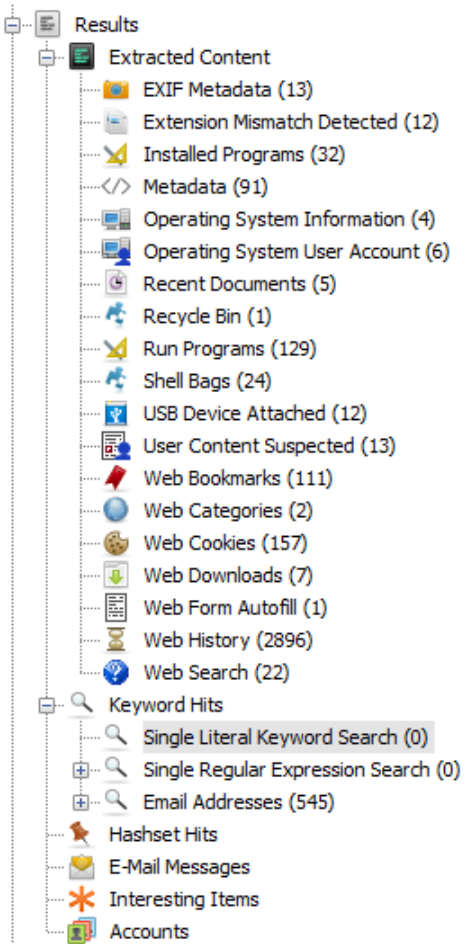


Ilustración 85 - Visualización de evidencia en Autopsy

5.2.5 Timeline

En el menú superior, una opción que suelo usar frecuentemente es la de “Timeline”, ya que todos los archivos son clasificados de acuerdo con los tiempos MAC (Modificación / Acceso / Creación), esto es útil cuando existió por ejemplo un hackeo en un día y hora determinada, y con esta herramienta podemos comenzar a visualizar que otros archivos, logs, o lo que fuere en ese momento o previamente fue modificado.

Ilustración 86 – Timeline en Autopsy

Timeline demora en clasificar los datos, por lo que debemos de estar conscientes que, al ejecutar esta opción, Autopsy Forensic nuevamente entrará en un modo en el que consume casi la totalidad de los recursos del procesador.

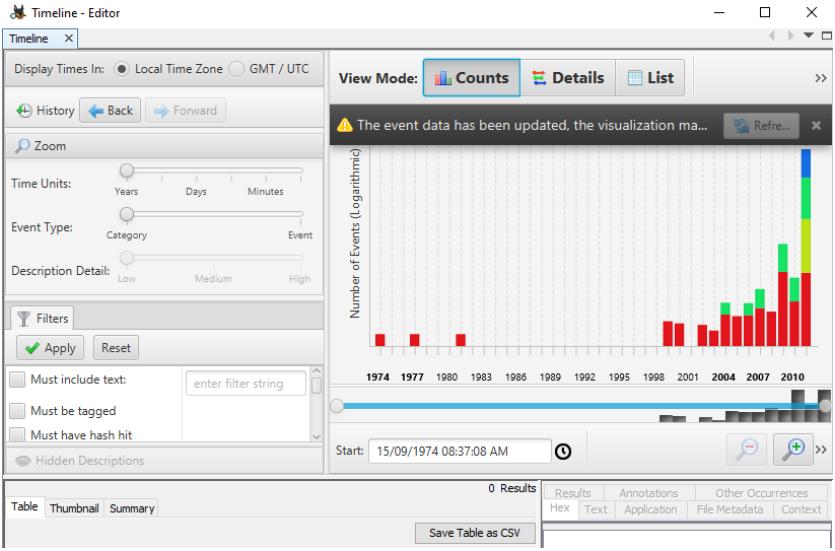


Ilustración 87 – Timeline en Autopsy

5.3 Suite forense comercial

En lo que respecta al software comercial podremos encontrar que hay opciones que van desde pocos dólares hasta miles y en miles llegamos a números que pueden superar los cientos (licencias multi usuarios destinados a gobiernos o corporativos muy grandes), pero iniciemos con las principales marcas y conozcamos sus ventajas.

De las empresas que llevan más tiempo en el mercado podremos encontrar a EnCase, FTK, Magnet Axiom, Nuix Workstation que tienen un enfoque principal para equipos de cómputo y por otra parte Cellebrite, Oxygen Forensic,

MobilEdit que se destinan principalmente para dispositivos celulares, aclaro que hago énfasis en “principalmente” ya que muchos fabricantes comenzaron a desarrollar módulos dentro de sus programas o software independiente destinados para cubrir otras áreas, sin embargo he probado la mayoría de ellos y los resultados son a mi parecer con un largo trayecto aun por maduración, salvo Cellebrite que sus programas tienen una muy alta eficiencia.

Debido a que no es intención de en este libro de parafrasear lo que los respectivos autores dicen de cada uno de los programas mencionados, daré un enfoque de lo que en términos generales pueden llevar a cabo las herramientas comerciales.

- **Soporte técnico**

Empecemos por mencionar que tendremos soporte técnico ante una falla del programa por parte de una empresa, al momento de llevar a cabo nuestras investigaciones, lo cual cambia por completo lo que en Autopsy Forensic tendríamos que resolver en los foros de ayuda, cada vez que el programa falle o tengamos un inconveniente con el software podemos ir con el fabricante y la atención es muy rápida, sin embargo, los valores agregados que estas empresas aportan son también.

- **Velocidad**

La robustez de los módulos que tienen incorporados, ya que podremos no solo clasificar la evidencia como lo pueden hacer las herramientas gratuitas, sino que además se máxima el uso del hardware, esto es crucial cuando tenemos un flujo de trabajo constante, los fabricantes dedican mucho tiempo a que el programa use al máximo el procesador, la memoria RAM y los discos duros que contienen las bases de datos, con ello el tiempo de procesamiento de la evidencia pueda finalizar en un tiempo muy por debajo de lo que el software gratuito consigue.

- **Clasificación con IA**

Otro punto muy interesante es la tecnología de Inteligencia Artificial que incorporan algunos fabricantes, ya que solo es necesario cargar la evidencia, habilitar la opción de IA e indicarle al programa que es lo que queremos clasificar, por ejemplo drogas, armas, desnudos, pornografía, violencia, vehículos, tarjetas de crédito, capturas de celular, detección OCR, entre otros módulos, lo que ayuda en gran medida a que el investigador tenga a un clic no miles de archivos, sino información de relevancia altamente clasificada.

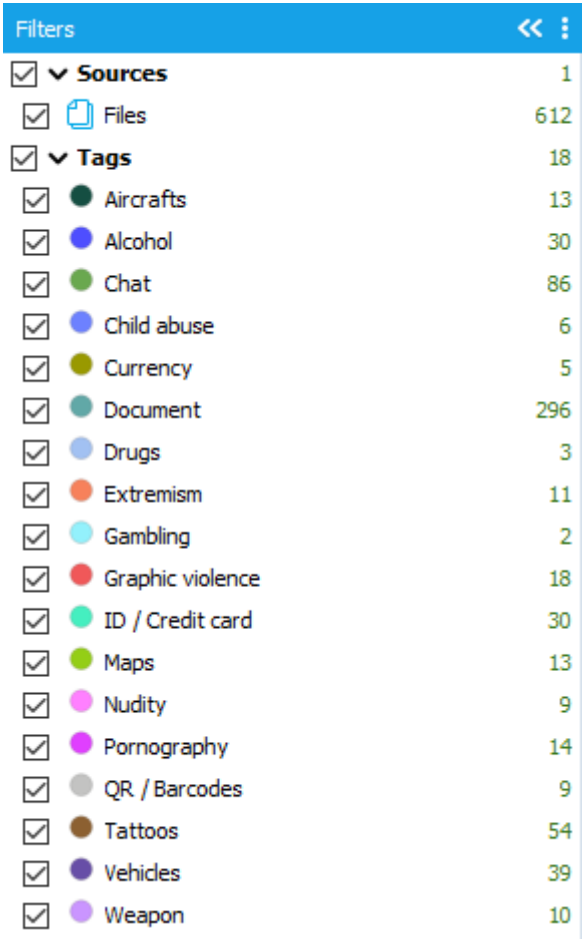


Ilustración 88 - Clasificación de evidencia con IA

- **Visualización de múltiples formatos**

Cuando hemos analizado millones de datos, lo cual es común con una copia forense de unos 250 Gb, tenemos clasificados diversos ficheros, sin embargo, en

herramientas como Autopsy Forensic, solo podemos visualizar el archivo en hexadecimal, vista gráfica (si es imagen o PDF) y vista hexadecimal, lo cual al tener archivos de un formato distinto, tenemos dificultad para analizarlo, para ello debemos exportar desde Autopsy uno a uno de los archivos hacia otro medio de almacenamiento que nos resultan interesantes para su correcta visualización, esto desde las herramientas comerciales se resuelve en la mayoría de los casos, ya que al navegar en la evidencia, podremos ir seleccionando archivos y el programa se encarga de mostrarnos una correcta visualización, por ejemplo, tablas de Excel, historial de navegación con opciones de filtrado y ordenado de datos y así con la mayoría de los formatos principales.

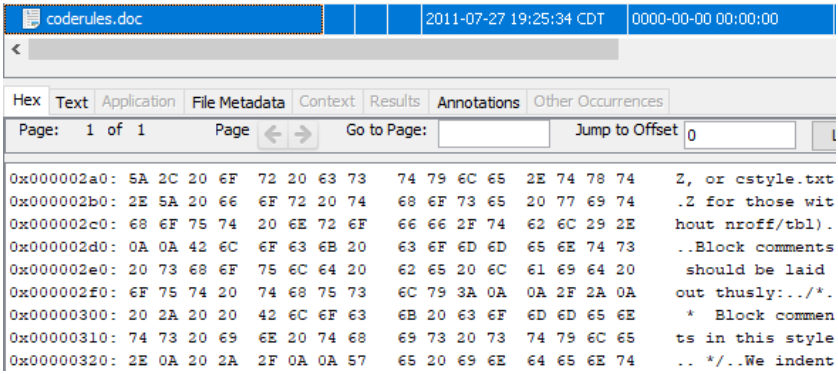


Ilustración 89 - Clasificación de evidencia con IA

- **Ataques de fuerza bruta**

Cuando existen archivos cifrados en la evidencia digital, tanto herramientas gratuitas como comerciales logran detectar dichos ficheros, la diferencia significativa es que las herramientas comerciales te permiten realizar ataques de fuerza bruta para romper la contraseña, uno podría pensaría que con una herramienta como JohnTheRipper se puede hacer lo mismo y no es así, las herramientas comerciales, por poner un ejemplo, como PRTK-DNA de AccesData, el cual consiste en un software con ataques de fuerza bruta con procesamiento distribuido, el cual nos permite además de el uso de tarjetas gráficas, crear un grupo de equipos de cómputo que se coordinarán entre ellos, sumando sus recursos de hardware, potenciando el ataque, además de los distintos perfiles para realizar ataques de fuerza bruta muy específicos y claro, cuentan con diccionarios muy robustos.

6.- Investigación digital sobre Windows

Como ya hemos hablado en capítulos previos, las investigaciones de informática forenses están focalizadas en poder tener una copia integra del dispositivo de cómputo sobre el cual se llevará a cabo el análisis (o lo más cercano que las posibilidades lo permitan), para poder trabajar sobre dicha copia y no comprometer en nuestros procesos de análisis la evidencia digital original, por ello la copia forense resulta fundamental dentro del área.

6.1 Agregar evidencia

Al tener una copia en formato dd, E01, AFF o el formato que hayamos seleccionado al momento de realizar la copia, viene acompañado de la pregunta ¿cómo interpreto esta información?, para ello distintas herramientas nos permiten interpretar estos datos, por ejemplo, en el caso de FTK con el que ya hemos trabajado, es similar al proceso descrito en el tema 4.7.1, sin embargo, el único cambio es al momento de agregar la evidencia, en lugar de seleccionar “Physical Drive” debemos seleccionar “Image File”, y la herramienta nos pedirá el archivo correspondiente a la copia forense, en el caso que estuviera fragmentado, solo debemos indicar el primer archivo y el programa se encarga de virtualmente unir las partes de la copia forense.

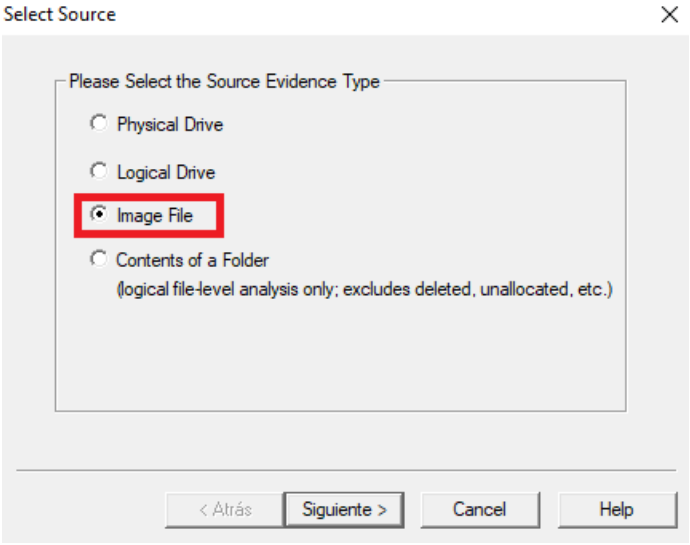


Ilustración 90 - Agregar evidencia con FTK

El resultado es un listado y navegación del contenido.

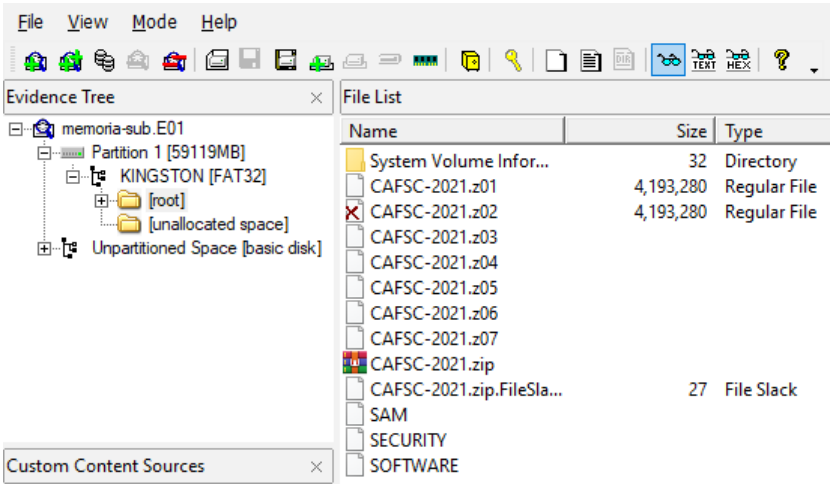


Ilustración 91 - Agregar evidencia con FTK

Que adicionalmente podremos extraer hacia donde nos sea conveniente, los archivos o directorios completos que nos sean de interés, con solo dar clic derecho y seleccionar “Export Files…”

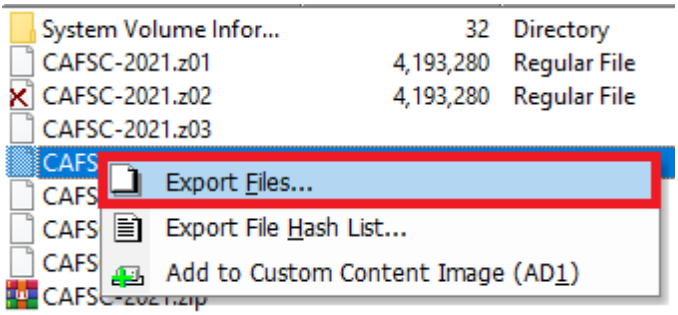


Ilustración 92 - Agregar evidencia con FTK

Una alternativa sería OSForensic, el cual tiene los siguientes pasos:

1. Debemos crear un nuevo caso desde el menú principal.

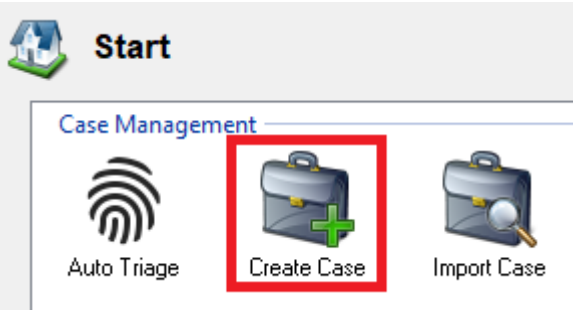


Ilustración 93 - Agregar evidencia con OSForensic

2. Posteriormente en la opción “Add Device”, debemos seleccionar “Image File” y la ruta donde se encuentra la copia forense.

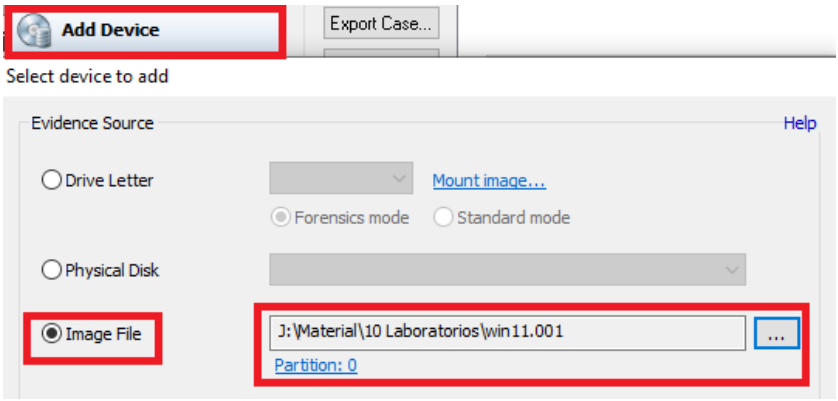


Ilustración 94 - Agregar evidencia con OSForensic

3. Con ello, ya tendremos en el menú “File System Browser”, la copia forense agregada y podremos navegar por los directorios y el acceso a los archivos, con las mismas funciones de extracción como las descritas para el FTK.

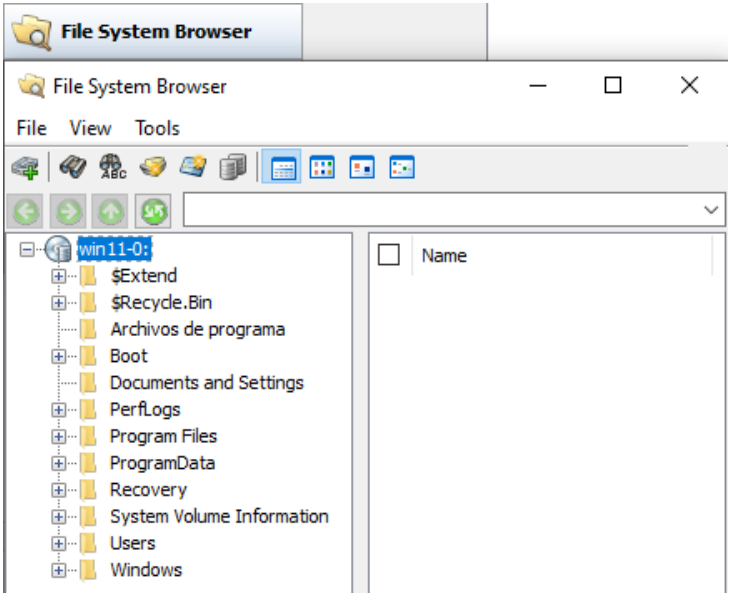


Ilustración 95 - Agregar evidencia con OSForensic

6.2 Montaje de copias forenses

El montaje de una copia forense es similar al agregar una copia forense como evidencia, ya que nos permite interpretar los datos de la copia, la diferencia radica en que en lugar de ver los archivos desde el programa forense, podremos usar nuestro explorador de Windows para trabajar sobre una unidad como si estuviera conectado físicamente un disco duro.

El proceso es similar en concepto a lo que programas muy comunes como Alcohol 120%, UltraISO, Nero Burning ROM nos permitían al virtualizar un archivo .iso

La empresa que desarrolló OSForensic, tiene un aplicativo gratuito llamado OSFMount el cual es bastante intuitivo con los siguientes pasos:

1. Una vez abierta la aplicación, debemos seleccionar “Mount new”

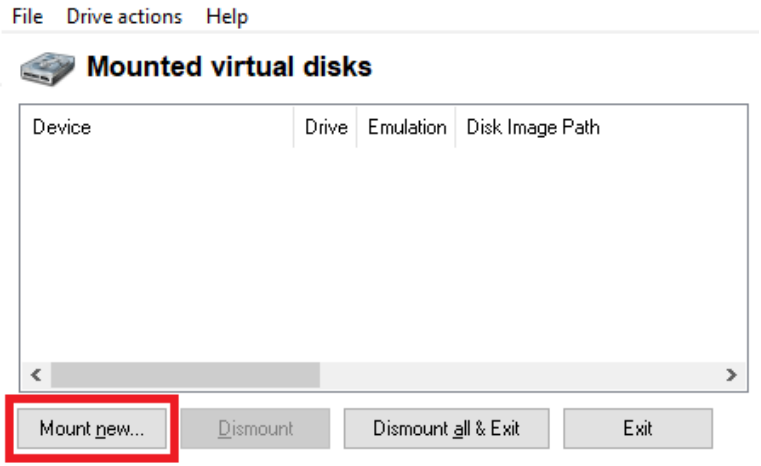


Ilustración 96 - Montaje de copias forenses con OSFMount

2. El sistema nos abre una nueva ventana la cual nos solicita la ruta de la copia forense, vale la pena señalar que tiene una gran compatibilidad con formatos de copias, así como con archivos de maquinas virtuales.

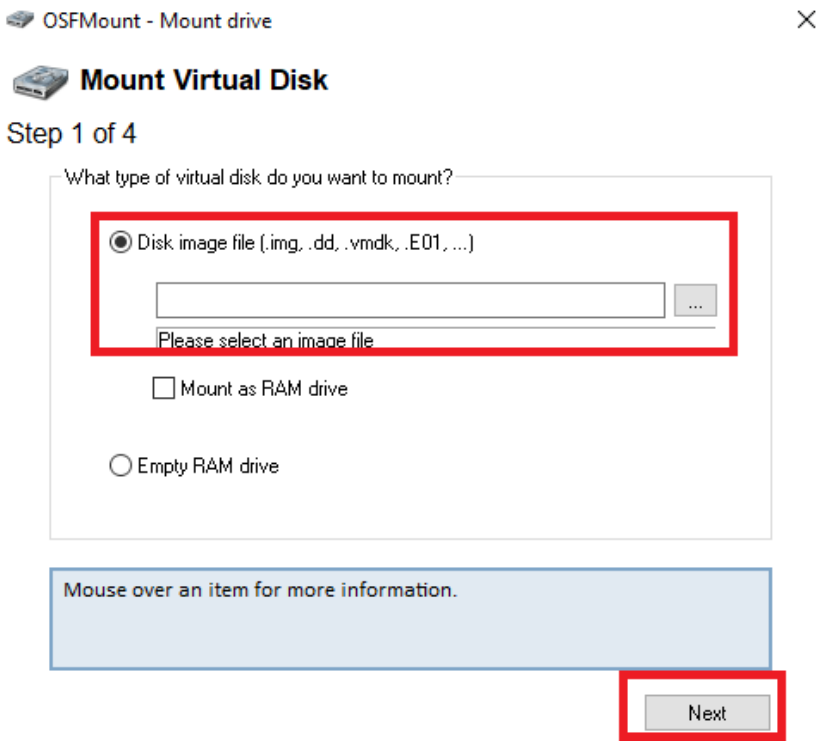


Ilustración 97 - Montaje de copias forenses con OSFMount

3. Nos pregunta el sistema ¿cuál de las particiones queremos montar?, para ello, si tenemos una copia forense de un sistema Windows, veremos que existen múltiples particiones y salvo que se requiera para un caso muy puntual, solo se debe seleccionar la partición del sistema operativo, sin marcar la opción “mount entire image as virtaul disk”

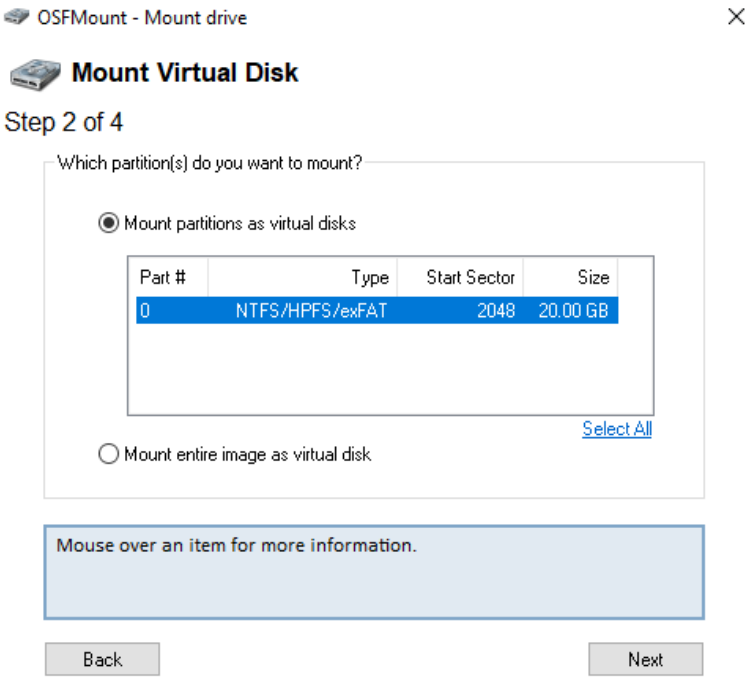


Ilustración 98 - Montaje de copias forenses con OSFMount

4. El último paso sería si queremos que sea montado en solo lectura, lectura/escritura y el tipo de emulación.

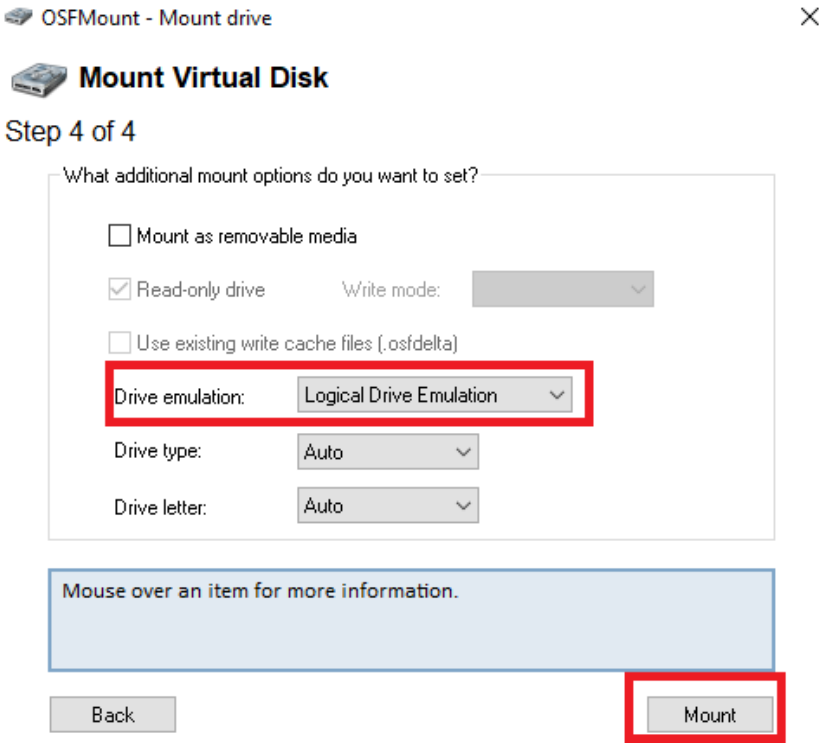


Ilustración 99 - Montaje de copias forenses con OSFMount

El resultado sería una unidad virtual totalmente accesible a todos los archivos.

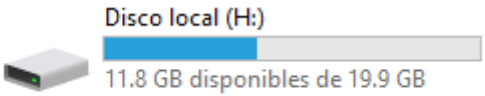


Ilustración 100 - Montaje de copias forenses con OSFMount

En este punto más de uno se preguntará, ¿pero que beneficio aporta el montar una unidad frente a solo agregarla como evidencia? La respuesta es todas las aplicaciones que conocemos que no trabajan sobre copias forenses, ahora pueden acceder y analizar esta unidad, por ejemplo, desde algo tan básico como un programa que recupera archivos eliminados, siempre como primer paso, debemos indicar el disco que se desea analizar, con este procedimiento de montado de unidad, podremos indicar el disco “H:” o la letra de la unidad que hayamos montado, ya que no trabajan con copias forenses, pero no solo recuperar archivos, herramientas forenses de análisis de logs, historiales de navegación, análisis de archivos de sistema, todo es ahora accesible.

6.3 Usuarios existentes

Un archivo que nos resulta muy importante es el SAM, que lo encontramos en C:\Windows\System32\config\ este archivo nos permite conocer localmente los usuarios que están registrados en el equipo de cómputo, pero además conocer datos importantes como: si la cuenta está activa, el último cambio de contraseña, último inicio de sesión, número de veces que se ha puesto mal la contraseña.

Para poder analizarlo, primero que nada, debemos saber que de una maquina Windows encendida no podemos interpretarlo, lo ideal es extraerlo de una copia forense, una vez que ya extrajimos el archivo con alguno de los métodos que vimos previamente, debemos realizar la interpretación de este, ya que, de abrirlo con un editor de texto como Bloc de notas, veremos que los datos no están en texto plano.

Una herramienta que me agrada por su alta compatibilidad es “Registry Viewer” de AccesData, vale la pena señalar que esta herramienta nos pide la licencia del software y en caso de no tenerla, podemos seguir adelante seleccionando “modo demo”.

La herramienta es muy simple por lo que el procedimiento sería:

1. Abrir el archivo “SAM”

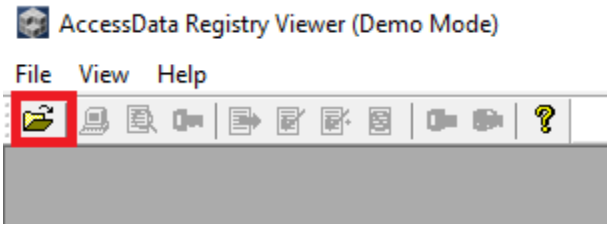


Ilustración 101 – Analizando el SAM con Registry Viewer

2. Debemos ir a la ruta SAM/Domains/Account/Users

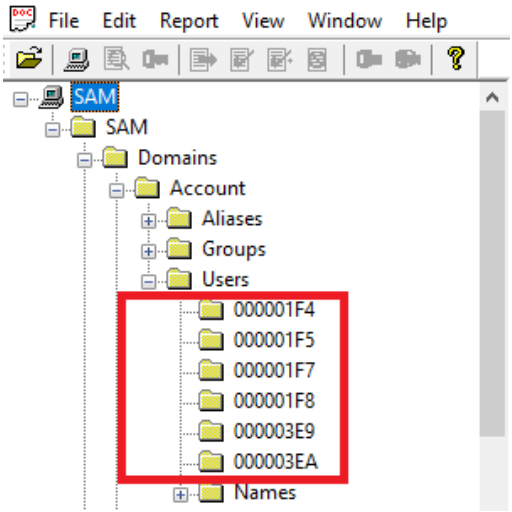


Ilustración 102 – Analizando el SAM con Registry Viewer

Al seleccionar uno a uno de los registros, podremos ver en la parte inferior la respectiva interpretación de los datos, en donde se desglosa la fecha de última escritura, el SID (número de identificación único), número de inicios de sesión, último cambio de contraseña entre otros datos.

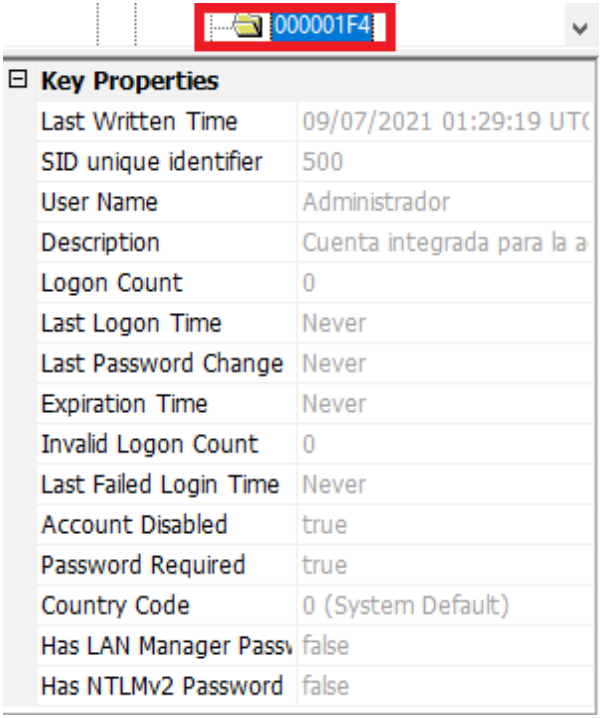


Ilustración 103 – Analizando el SAM con Registry Viewer

Los valores de SID que se encuentran en el rango de 500 corresponden a usuarios que el sistema operativo creó, aquí podemos encontrar una cuenta de administrador 500 y una de invitado 501 que vienen en todos los sistemas Windows, sin embargo, están de forma nativa deshabilitadas, valdría la pena por ejemplo, verificar si la cuenta 500 fue habilitada en algún momento ya que es muy frecuente encontrar esto en casos de hackeos a servidores de empresas, en donde alguien, interno o externo llegó a

habilitar la cuenta sin que se muestre dentro del panel de control de Windows.

6.4 Hosts

Para entender la importancia de este archivo, debemos comprender que al colocar en nuestro navegador una dirección como www.google.com este no entiende de direcciones y necesita saber cual es la IP de Google para conectarse, para ello el primer paso es consultar en caché si se cuenta con el registro de esta ip, en caso contrario verifica en el archivo “hosts” si está definida la IP de www.google.com en caso que si estuviera definida, se conecta a esta dirección, en caso contrario se realizan consultas al router, a nuestro ISP y a los registrantes de dominios para conocer este dato, sin embargo nosotros nos quedamos en el punto del archivo hosts, es ahí donde un atacante pudo haber definido una ip quizá no para www.google.com pero podría ser para la página de un banco, una red social o un sitio que sea su objetivo, también puede ser el caso que el administrador de sistemas está bloqueando redes sociales o dominios que son de interés y así los empleados de una empresa no pueden acceder a páginas específicas.

En la ruta C:\Windows\System32\drivers\etc podremos encontrar el archivo “hosts”, el cual podremos abrir con cualquier editor de textos.

Un archivo limpio, debería mostrarse de la siguiente forma.

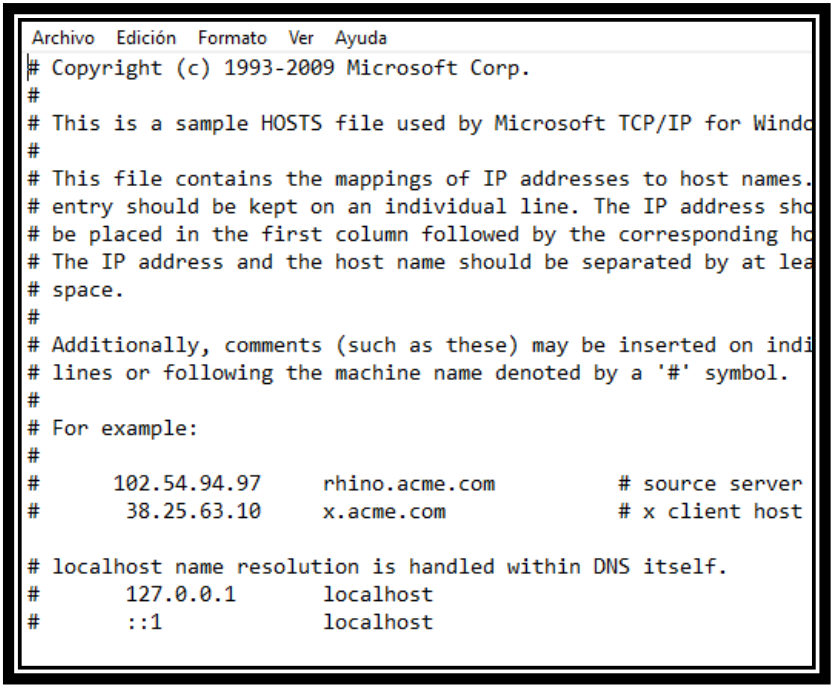
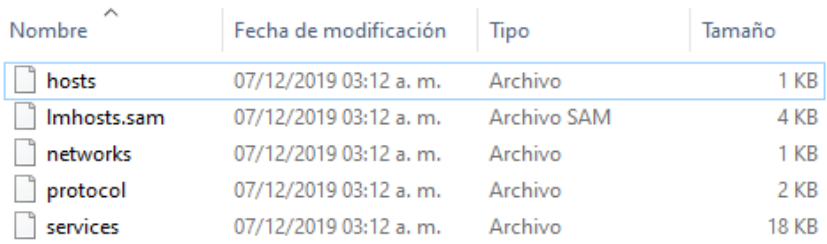


Ilustración 104 – Hosts de Windows

En donde no exista un valor a dominios específicos, sin embargo, esto no garantiza que no ha sido modificado, por ello siempre reviso la fecha y hora de modificación, en donde los valores en una instalación limpia de Windows coinciden los archivos de dicha carpeta, en caso que

encontremos que se han manipulado debe ser una llamada de atención de que hay algo extraño.



Nombre	Fecha de modificación	Tipo	Tamaño
hosts	07/12/2019 03:12 a. m.	Archivo	1 KB
lmhosts.sam	07/12/2019 03:12 a. m.	Archivo SAM	4 KB
networks	07/12/2019 03:12 a. m.	Archivo	1 KB
protocol	07/12/2019 03:12 a. m.	Archivo	2 KB
services	07/12/2019 03:12 a. m.	Archivo	18 KB

Ilustración 105 - Hosts de Windows

Una explicación a un cambio en estos archivos, se da con frecuencia cuando se instaló software sin licencia y se ejecutó un activador, estos programas suelen modificar el archivo hosts para evitar que el programa pueda validar la clave o reciba actualizaciones.

6.5 Eventos del sistema

Los eventos de Windows tienen una carpeta definida la cual encontramos en C:\Windows\System32\winevt\Logs, pero el administrador de sistemas puede sin mayor problema mover la ruta de los eventos por lo que valdría la pena analizar las llaves de Windows siguientes para detectar si se cambiaron las rutas originales.

HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application

HKLM\SYSTEM\CurrentControlSet\Services\EventLog\System

HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security

Los archivos originalmente son con formato .evt los cuales eran binarios, sin embargo, en la actualidad el formato es .evtx, el cual nos da muchas mejoras al momento de realizar búsquedas.

Para interpretar estos archivos, el propio sistema operativo Windows lo realiza, por lo que no es menester contar con aplicaciones de terceros, pero las aplicaciones de terceros permiten no solo abrir los archivos, sino aplicar filtros de acuerdo con el nivel de riesgo de los eventos.

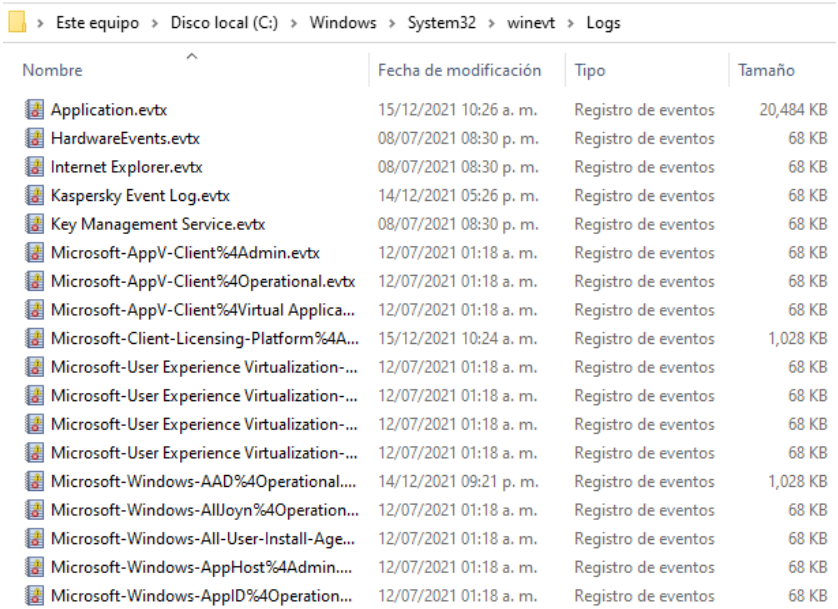


Ilustración 106 - Eventos del sistema Windows

La herramienta OSForensic, en el apartado “Event Log Viewer” tiene una serie de filtros que nos ayudan a filtrar entre miles de eventos del sistema.

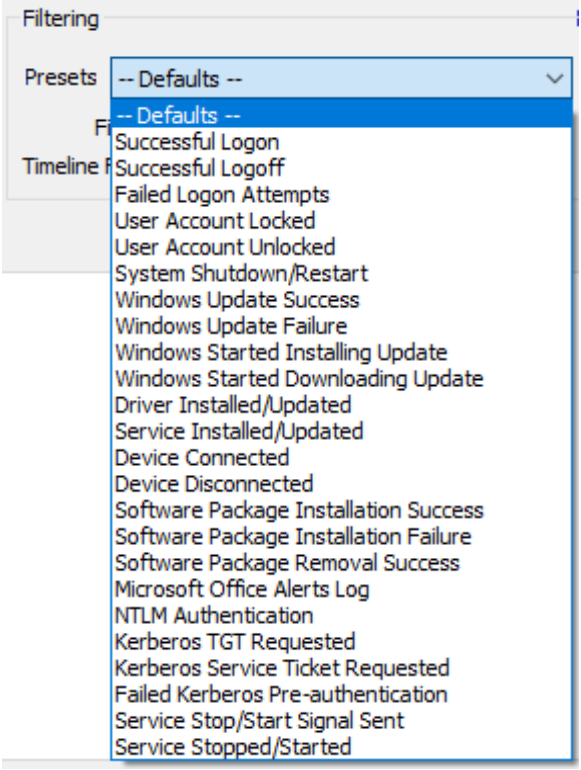


Ilustración 107 - Eventos del sistema Windows con OSForensic

6.6 Prefetch

Los sistemas Windows contienen un servicio el cual precarga las principales aplicaciones que se ejecutan, este

servicio almacena los datos en C:\Windows\Prefetch y para poder analizar los datos vamos a requerir de programas destinados para ello.

La relevancia de este servicio es que contiene un listado de las aplicaciones, por ejemplo WinWORD.exe, el cual es el ejecutable de Word, si analizamos el prefetch de WindWord.exe, podremos obtener un listado de los archivos que fueron abiertos mediante Word, en este caso se hizo uso de WinPrefetchView v1.37.

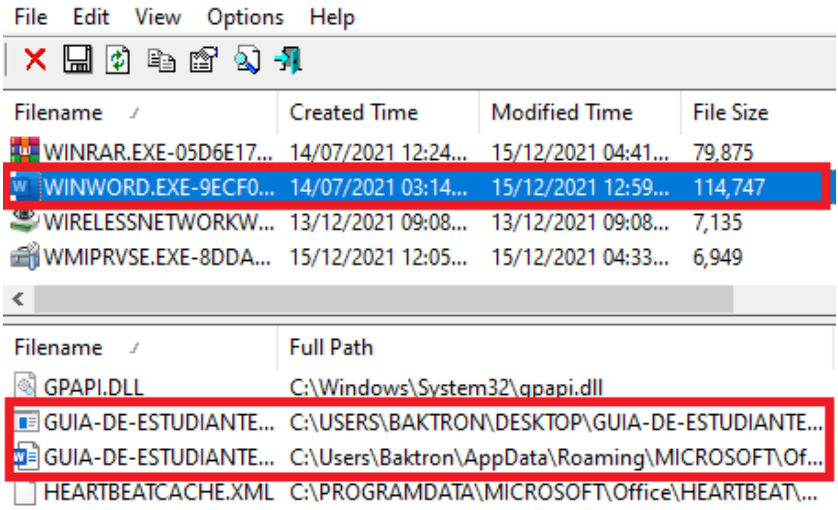


Ilustración 108 - Prefetch

Esto resulta adicionalmente útil cuando un usuario ha ejecutado una aplicación que elimina su historial de actividad, ya que la carpeta prefecth no se elimina con las configuraciones estándar de los programas de eliminado,

por ello siempre vale la pena echar un vistazo sobre aplicaciones que nos son de relevancia.

Otro ejemplo es explorer.exe, el cual nos dice que se ha abierto Word, Excel, OSForensic y Oxygen Forensic, pero no nos indica la fecha en se abrieron dichos programas, solo nos confirma la apertura de estos.

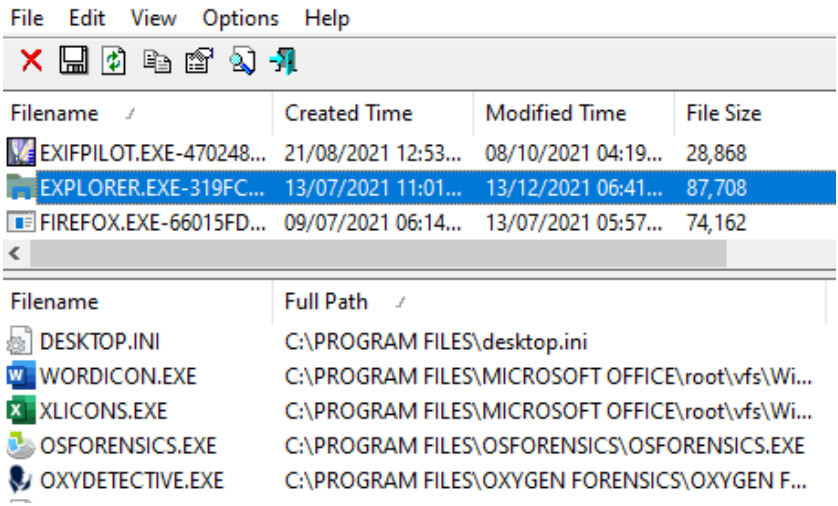


Ilustración 109 - WinPrefetchView

6.7 Shadowcopy

Los sistemas operativos Windows realizan de forma automática “instantáneas” de los archivos, los cuales son

útiles cuando llega una actualización o se instala un programa que causa problemas y se requiere volver a una versión previa, esto es algo que podemos usar cuando un Ransomware atacó y cifró los archivos, con suerte se pueden recuperar documentos que estén en estas instantáneas, aunque diversas familias de ransomware son consciente de ello y suelen ir a buscar las instantáneas y eliminar el contenido.

Para acceder a las instantáneas, solo debemos colocar el comando “vssadmin list shadows” desde CMD con permisos de administrador, el resultado debe ser como el siguiente.

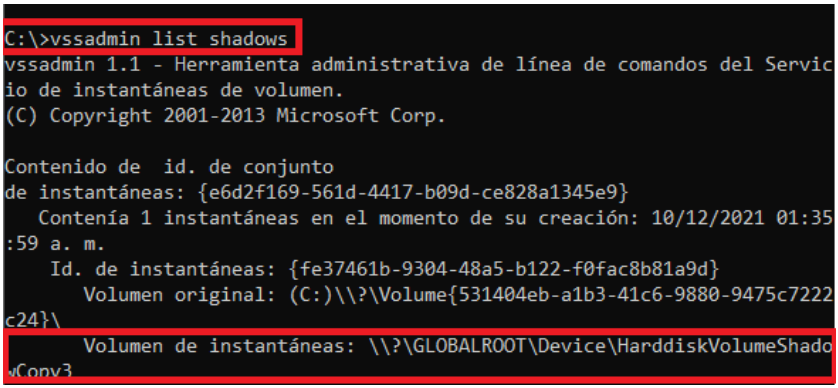


Ilustración 110 - Shadowcopy

Es posible que el sistema “no encontró elementos que cumplen con dicha característica”, lo cual se interpreta como que dicho disco no cuenta con instantáneas, esto se

debe a que se deshabilitó el espacio para dichas instantáneas, que podría ser una forma de ahorrar espacio en disco.

De lo que nos indica el comando, nos interesa conocer la ruta de las instantáneas que se detectaron, las cuales tienen la siguiente sintaxis

\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3

Para poder acceder al contenido de dicha instantánea, debemos crear un enlace simbólico, lo cual podemos hacer de la siguiente forma:

mklink /d C:\ruta-del-link \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\

En el ejemplo creo un enlace simbólico en C: con el nombre de “shadow1”

```
C:\>mklink /d C:\shadow1 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\
vínculo simbólico creado para C:\shadow1 <<===>> \\?\GLOBALROOT\Device\Har
ddiskVolumeShadowCopy3\
```

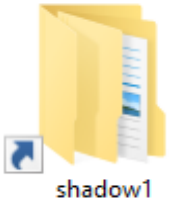


Ilustración 111 - Shadowcopy

Al acceder a esta mencionada carpeta, veré una estructura similar a estar en C:\ pero al navegar en las carpetas documentos, descargas, escritorio o diversas carpetas del usuario, podremos encontrar archivos que habían sido eliminado hace tiempo.

6.8 MFT

Los sistemas de archivos NTFS (Windows) manejan un directorio con el registro de todos los archivos que se han llegado a almacenar a lo largo del tiempo (cada que se formatea la unidad se elimina y se crea uno nuevo registro), el registro como tal es el archivo “$MFT”, el cual encontraremos en la unidad raíz de la partición, su relevancia a nivel forense es que puede pasar el tiempo pero podemos conocer los archivos que se han llegado a tener, no importa si fue ejecutada una aplicacióno que elimina historial de actividad como Cclener, el archivo $MFT no elimina el nombre del archivo que se tuvo.

Para el caso estoy usando Mft2Csv, la cual es totalmente libre y tiene una interfaz gráfica bastante potente.

Podemos escanear los discos existentes, las particiones o cargar directamente un archivo $MFT, solo esto es necesario para que la herramienta comience con el proceso de interpretación y nos arroje archivos .csv que

podremos abrir y aplicar los filtros y orden de columnas que más nos resulten importantes.

Un ejemplo de uso es poder detectar si un empleado ha tenido un archivo que la empresa sospecha pudo almacenar, detectar los archivos que fueron modificados, editados o creados en un rango de tiempo determinado, como previo a un hackeo o posterior a ello.

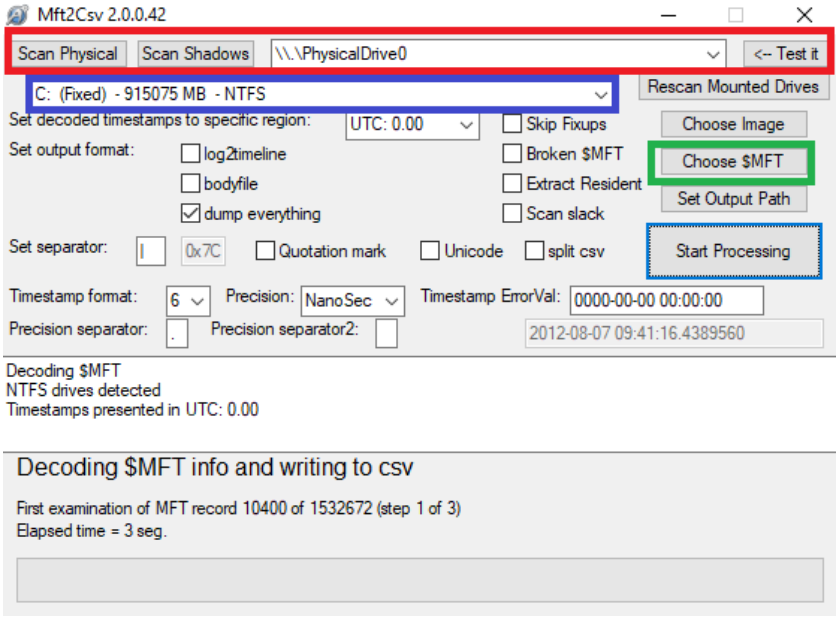


Ilustración 112 - MFT

Los archivos .csv se van a crear en la misma carpeta en donde se encuentra nuestra herramienta, salvo que le indiquemos al programa una ruta en específico.

7.- Análisis a la RAM

Como se mencionó al inicio, parte de nuestra labor como expertos en informática forense y dentro del proceso mismo descrito, llevamos a cabo la preservación de evidencia, es aquí donde la memoria RAM tuvo que haber sido copiada para no perder esos gigas de información que al apagarse el equipo se perderían.

El tema ahora es ¿cómo analizar estos datos? Si es una copia forense, ¿podemos analizarla desde herramientas previas?, ¿qué tanta información podremos encontrar?

Veremos que la memoria RAM resulta maravillosa en el proceso de análisis ya en nuestro laboratorio, tener este archivo nos dará acceso a mucha información y datos precisos que estaban mientras el equipo de cómputo estuvo encendido.

7.1 Volatility

De las herramientas que existen, la que más destaca es Volatility, de hecho, herramientas con interfaz gráfica para el análisis de la memoria RAM, son solo una GUI del propio Volatility, como el que tiene la herramienta OSForensic por mencionar algunos.

El proyecto de volatility es libre y multiplataforma, alrededor de este proyecto se han desarrollado muchas herramientas

que lo usan como el motor, por lo que es una herramienta bastante robusta y actualizada.

La sintaxis inicial de uso es:

volatility -f <ruta-del-archivo> <comando>

Sin embargo tendremos que incluir algo que se conoce como perfil, el cual será específico para cada análisis de memoria ram que llevamos a cabo, siendo la sintaxis siguiente.

volatility -f <ruta-del-archivo> <perfil> <comando>

7.1.1 Perfiles

Hasta la versión 2.6 de Volatility (la más extendida), debía primeramente analizar el volcado de memoria y debíamos indicar el corresponde a la versión del sistema operativo, cada versión de Windows ya sea Windows XP,Vista,7,8,8.1,10,11 Linux, MAC de 32/64 bits tiene una estructura de su memoria RAM, no es la misma estructura de la RAM en un Windows XP 32 bits que un Windows XP 32 bits SP2, de hecho, con cada actualización existen cambios en el sistema que afectan la estructura de la memoria RAM, por ese motivo, a Volatility tenía como primer paso el análisis del perfil para poder usarlo al momento de solicitarle nos muestra los procesos, servicios,

librería o cualquier dato que nos fuera de relevancia, con la versión 3 esto se acabó, y podemos directamente pedirle la información que nos interesa, la sintaxis es la siguiente:

vol.py -f <ruta-archivo> <que-buscamos>

Como es costumbre, podemos dar un “vol.py -h” para obtener ayuda y un listado de los argumentos que le podemos indicar al programa.

```
An open-source memory forensics framework

optional arguments:
  -h, --help            Show this help message and exit, for specific plugin
                        options use 'volatility <pluginname> --help'
  -c CONFIG, --config CONFIG
                        Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument
                        given)
  -e EXTEND, --extend EXTEND
                        Extend the configuration with a new (or changed)
                        setting
  -p PLUGIN_DIRS, --plugin-dirs PLUGIN_DIRS
                        Semi-colon separated list of paths to find plugins
  -s SYMBOL_DIRS, --symbol-dirs SYMBOL_DIRS
                        Semi-colon separated list of paths to find symbols
  -v, --verbosity       Increase output verbosity
  -l LOG, --log LOG     Log output to a file as well as the console
  -o OUTPUT_DIR, --output-dir OUTPUT_DIR
                        Directory in which to output any generated files
  -q, --quiet           Remove progress feedback
  -r RENDERER, --renderer RENDERER
                        Determines how to render the output (quick, csv,
                        pretty, json, jsonl)
```

Ilustración 113 - Volatility

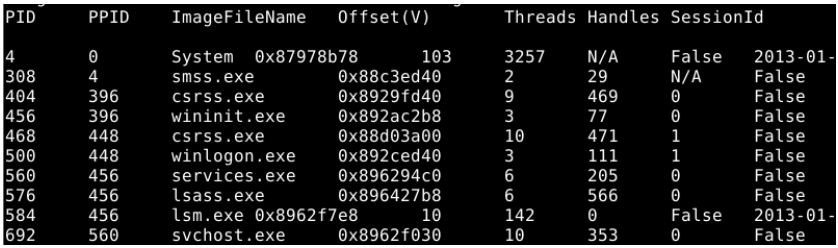
7.1.2 Procesos y subprocesos

El primer punto que se analiza, son los procesos que se estaban ejecutando cuando el equipo estaba encendido, es

muy similar a ver de un equipo el administrador de tareas, con la clara ventaja que podremos analizar a profundidad las bibiotecas que se estaban usando por cada uno de los precesos, la ruta del ejecutable, procesos padre e hijo. Vayamos a ello, con “python3 vol.py -f <ruta-archivo> windows.psscan.PsScan” se mandan a llamar todos los procesos y son listados uno a uno.

```
sudo python3 vol.py -f memoria.mem windows.psscan.PsScan
```

Nos devuelve el reporte con información muy valiosa, como los son: el nombre del proceso, PID, PPID además de la hora de ejecución.



PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	
4	0	System	0x87978b78	103	3257	N/A	False 2013-01-
308	4	smss.exe	0x88c3ed40	2	29	N/A	False
404	396	csrss.exe	0x8929fd40	9	469	0	False
456	396	wininit.exe	0x892ac2b8	3	77	0	False
468	448	csrss.exe	0x88d03a00	10	471	1	False
500	448	winlogon.exe	0x892ced40	3	111	1	False
560	456	services.exe	0x896294c0	6	205	0	False
576	456	lsass.exe	0x896427b8	6	566	0	False
584	456	lsm.exe	0x8962f7e8	10	142	0	False 2013-01-
692	560	svchost.exe	0x8962f030	10	353	0	False

Ilustración 114 – Volatility

Una alternativa es listar los procesos en forma de árbol, para tener gráficamente un reporte de el proceso padre y los procesos que se desprenden de este, el comando sería:

python3 vol . py -f <ruta-archivo> windows.pstree.PsTree

```
sudo python3 vol.py -f memoria.mem windows.pstree.PsTree
```

```
PID      PPID     ImageFileName   Offset(V)          Threads Handles

4        0        System  0x87978b78      103      3257    N/A
* 308    4        smss.exe        0x88c3ed40       2       29
404      396      csrss.exe       0x8929fd40       9       469
456      396      wininit.exe     0x892ac2b8       3       77
* 560    456      services.exe    0x896294c0       6       205
** 904   560      svchost.exe     0x89852918       17      409
*** 2496          904     dwm.exe 0x87ad44d0       5       77
** 1172  560      svchost.exe     0x898b2790       15      475
** 3352  560      svchost.exe     0x89f3d2c0       9       141
** 928   560      svchost.exe     0x8986b030       26      869
** 3624  560      svchost.exe     0x89f1d3e8       14      348
** 1712  560      spoolsv.exe     0x8a0f9c40       14      338
** 1968  560      vmtoolsd.exe    0x8a1d84e0       6       220
** 2352  560      taskhost.exe    0x87ac0620       8       149
** 692   560      svchost.exe     0x8962f030       10      353
** 1084  560      svchost.exe     0x898911a8       10      257
** 448   560      VMUpgradeHelpe  0x8a1f5030       4       89
*** 468  448      csrss.exe       0x88d03a00       10      471
**** 2600         468     conhost.exe     0x87a9c288       1
**** 3228         468     conhost.exe     0x87c595b0       2
**** 2168         468     conhost.exe     0x954826b0       2
```

Ilustración 115 – Volatility PsTree

Por temas de una mejor visualización, en la imagen previa se recortó el resultado de volatility, sin embargo, hay columnas con información adicional.

7.1.3 Inspección de librerías usadas

Saber el nombre de un proceso que se ejecuta no nos dice mucho a nivel forense, podemos ver listado un proceso llamado “Explorer.exe”, el cual asociamos con la interfaz gráfica de un sistema Windows, sin embargo, en un ataque informático, se tiene muchas veces por objetivo que

procesos normales, tengan dentro de si un proceso malicioso o bien, estén usando bibliotecas que permiten a un atacante realizar diversas actividades, es por ello, que de un proceso debemos identificar las bibliotecas que se estaban usando, el comando sería:

python3 vol . py -f <ruta-archivo> windows.dlllist.DllList pid <número del proceso>

```
sudo python3 vol.py -f memoria.mem windows.dlllist.DllList --pid 1220
PID     Process Base    Size    Name    Path    LoadTime        File output

1220    AvastSvc.exe    0x320000        0xc000  AvastSvc.exe    C:\Program Files\AV
1220    AvastSvc.exe    0x77660000      0x13c000        -       -       N/A     Dis
1220    AvastSvc.exe    0x77480000      0xd4000 kernel32.dll    C:\Windows\system32\
1220    AvastSvc.exe    0x75920000      0x4a000 KERNELBASE.dll  C:\Windows\system32\
1220    AvastSvc.exe    0x777a0000      0x35000 WS2_32.dll      C:\Windows\system32\
1220    AvastSvc.exe    0x76a60000      0xac000 msvcrt.dll      C:\Windows\system32\
1220    AvastSvc.exe    0x76c10000      0xa1000 RPCRT4.dll      C:\Windows\system32\
```

Ilustración 116 – Volatility DllList

Del ejemplo, volatility nos listará las bibliotecas que el proceso 1220 estaba usando.

7.1.4 Extracción de ejecutables

De volatility, una de las opciones que nos aportan un valor incalculable, es el poder recuperar el proceso que estaba en la memoria RAM, para ello, podemos indicarle a volatility el proceso exacto que queremos tener disponible y nos

devolverá el archivo con dicho proceso, el comando requerido sería:

sudo python3 vol.py -f memoria.mem windows.pslist.PsList --pid 1220 --dump

```
forense@Tequila:~/volatility3$ sudo python3 vol.py -f memoria.mem
windows.pslist.PsList --pid 1220 --dump
Volatility 3 Framework 2.0.0
Progress:  100.00               PDB scanning finished

PID     PPID    ImageFileName   Offset(V)       Threads Handles Se
ssionId       Wow64   CreateTime      ExitTime        File output

1220    560     AvastSvc.exe    0x898a7868      66      1180    0
      False   2013-01-12 16:38:28.000000      N/A     pid.1220.0x
320000.dmp
```

Ilustración 117 – Volatility DllList

El archivo resultante podremos analizarlo de diversas formas, ya sea por nombrar algunos, OllyDbg, Ghidra, WinDbg, esto implica un conocimiento sólido en descompilar un archivo ejecutable, o bien, una alternativa rápida es subirlo a una sanbox de las gratuitas que están en internet, además de subirlo a virustotal.com para que diversos antivirus lo analicen e indiquen si es detectado como malicioso.

Índice de ilustraciones

Número	Descripción	Página
1 y 2	Colisión MD5	
3	Colisión MD5 demostración	
4	Colisión MD5 demostración	
5 y 6	Colisión SHA1	
7	Colisión SHA1 demostración	
8	Diferencias backup y copia forense	
9 y 10	Copia de la memoria RAM con FTK	
11 y 12	Copia de la memoria RAM con Live RAM Capturer	
13	Copia en Linux con dd	
14	Copia en Linux de la memoria RAM con dd	
15	Acceso a procesos /proc en Linux	
16	Listado de procesos en Linux	
17	Comandos de Windows aplicados a forense	
18	Protocolo ARP	
19	Historial de CMD	
20	Configuración de red	
21	Conexiones de red activas	
22	CurrPorts	
23	Tareas programadas	
24	Información del sistema	
25	Historial de navegación en Chrome	
26	Agave Forense	
27	WinTriage	
28	WinTriage opciones	
29	WinUFO	
30	Discos SATA vs SAS	
31	Discos SCSI	
32	Discos duros USB	
33	Discos duros PCIE	
34	Discos duros M.2	
35	Bloqueadores Tableau	
36	Bloqueadores Wiebetech	
37	Duplicador Tx1 de Tableau	

38	Data Copy King II de SalvationData	
39 - 46	Copia forense con FTK Imager	
47- 49	Copia forense con OSForensic	
50 y 51	Copia forense con HelixPro	
52	Listado de unidades y puntos de montaje en Linux	
53 y 54	Copia forense en Linux con dd	
55	Copia forense en vivo, sistemas Windows	
56	Detección de unidades cifradas con MAGNET	
57 - 62	Detección de unidades cifradas con FTK	
63 y 64	BitLocker	
65 y 66	Copia forense en vivo, entornos Windows cifrados	
67	Cálculo del valor hash desde CMD	
68	Cálculo del valor hash desde PowerShell	
69	Cálculo hash con Multihasher	
70 y 71	Cálculo hash con OSForensic	
72	Cálculo hash desde Linux	
73	Laboratorio forense	
74 y 75	Autopsy Forensic	
76 - 79	Crear un caso en Autopsy Forensic	
80	Módulos en Autopsy Forensic	
81 y 82	Procesamiento en Autopsy Forensic	
83 - 85	Visualización de evidencia en Autopsy	
86 y 87	Timeline en Autopsy	
88 y 89	Clasificación de evidencia con IA	
90 - 92	Agregar evidencia con FTK	
93 - 95	Agregar evidencia con OSForensic	
96 - 100	Montaje de copias forenses con OSFMount	
101 - 103	Ilustración 102 – Analizando el SAM con Registry Viewer	
104 y 105	Hosts de Windows	
106	Eventos del sistema Windows	
107	Eventos del sistema Windows con OSForensic	
108	Prefetch	
109	WinPrefetchView	
110 y 111	Shadowcopy	
112	MFT	

113	Volatility	
114	Volatility PsScan	
115	Volatility PsTree	
116	Volatility DllList	
117	Volatility Dump	

Credenciales para informática forense

Me es importante señalar que en cada país existen requisitos para poder desempeñarse y presentarse ante un juez como perito en materia de informática forense, en la mayoría de los casos se acredita con diplomados o certificaciones, en México, por ejemplo, hay estados que piden un grado de licenciatura en alguna ingeniería y otros estados no lo exigen.

En cuanto a cursos, diplomados o certificaciones que conozco de primera mano son por orden alfabético:

Duriva. La certificación que se imparte es: Computing Analysis Forensics Specialized Certification (CAFSC), modalidad online y presencial (un servidor imparte la totalidad del curso).

SANS. Existen diversos niveles, en promedio el cada curso tiene una duración de 40 horas, modalidad online y presencial.

Securízame. La certificación que se imparte es: Digital Forensic & Incident Response (DFIR), modalidad online y presencial, en su totalidad tiene una duración de 90 horas, aunque es posible acceder a módulos puntuales.

Laboratorios Forenses

Me es importante señalar que en cada país existen requisitos para poder desempeñarse y presentarse ante un juez como perito en materia de informática forense, en la mayoría de los casos se acredita con diplomados o certificaciones, en México, por ejemplo, hay estados que piden un grado de licenciatura en alguna ingeniería y otros estados no lo exigen.

- El American Council For Cybersecurity And Computer Forensic (ACCCF) tiene laboratorios de práctica.
  https://americancybersecurity.org/laboratorios

- Los ejercicios de este libro se podrán replicar en una maquina virtual que estará en: https://jocsanlaguna.com/laboratorios

Descargo de responsabilidad

Las marcas nombradas en el presente libro les pertenecen a sus respectivos dueños y fueron usados sus nombres e imágenes con fines educativos y de ilustración.

Atribución-NoComercial 4.0 Internacional

FUNDAMENTOS DE LA INFORMÁTICA FORENSE

POR: JOCSAN LAGUNA

Jocsan Laguna
CEO

Partiendo de los fundamentos teóricos, nos adentraremos en el mundo de la informática forense con un enfoque altamente práctico y lleno de ejemplos para cada uno de los temas, añadiendo comentarios y recomendaciones de lo que he sintetizado en más de 13 años de experiencia y la transferencia de conocimientos que he brindado a fuerzas del orden como a la Policía de Buenos Aires y Chaco, Carabineros de Chile, Policía Nacional de Colombia, Policía Nacional del Perú, AGETIC en Bolivia, Policía Nacional del Ecuador, Fuerza Pública de Costa Rica, así como Policías Cibernéticas, Fiscalías y elementos del CISEN y de la SSC de México.

Jocsan Laguna
CEO

duriva